WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Wednesday, April 27, 2005

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=OR	
☐	L23	19990101	6
☐	L22	l3 and manufactur$5 near10 (device$1 or player$1 or set$1top or stb) with generat$4 near10 (public or private)	12
☐	L21	l3 and manufactur$5 near10 (device$1 or player$1 or set$1top or stb)	228
☐	L20	19990701	14
☐	L19	l3 and tempor$4 near10 (public or private)	22
☐	L18	(seed or device adj identifier) with manufactur$4 with licens$4 with (temporar$4 or first or initial) with (private or public)	0
☐	L17	key adj information with manufactur$4 with licens$4 with (temporar$4 or first or initial) with (private or public)	0
☐	L16	5805712.pn.	1
☐	L15	6088797.pn.	1
☐	L14	5774552.pn.	1
☐	L13	5557518.pn.	1
☐	L12	5233505.pn.	1
☐	L11	5159629.pn.	1
☐	L10	5159629.pn.	1
☐	L9	4860351.pn.	1
☐	L8	6233685[uref]	0
☐	L7	4218582.pn.	1
☐	L6	6233685.pn.	1
☐	L5	L3 and manufactur$4 with (device$1 or set$1top or player$1) with (tempora$5 or initial or first) with (key$1 or public or private)	12
☐	L4	L3 and manufactur$4 with (device$1 or set$1top or player$1) with (tempora$5 or initial or first) with (key$1 or public or private) with (seed or key adj information or device adj identifier or initial adj key)	2
☐	L3	L2 or l1	2608
☐	L2	380/211,278.ccls.	278
☐	L1	713/201,156,175,193,194.ccls.	2383

END OF SEARCH HISTORY

```
File   8:Ei Compendex(R) 1970-2005/Apr W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Mar
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Apr W4
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Apr W3
         (c) 2005 Institution of Electrical Engineers.
File  94:JICST-EPlus 1985-2005/Mar W2
         (c)2005 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2005/Apr W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Apr W3
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Apr W3
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Mar
         (c) 2005 The HW Wilson Co.
File 266:FEDRIP 2005/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Mar W3
         (c) 2005 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2005/Feb
         (c) 2005 The HW Wilson Co
File  62:SPIN(R) 1975-2005/Feb W1
         (c) 2005 American Institute of Physics
File 239:Mathsci 1940-2005/Jun
         (c) 2005 American Mathematical Society
File 347:JAPIO Nov 1976-2004/Dec(Updated 050405)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200526
         (c) 2005  Thomson Derwent
File 348:EUROPEAN PATENTS 1978-2005/Apr W03
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050421,UT=20050414
         (c) 2005 WIPO/Univentio

Set     Items   Description
S1      18179   (PRIVATE OR SECRET)(1W)KEY? ?
S2         94   (TEMPORARY OR TRANSIENT OR INTERMEDIATE OR TRANSITIONAL OR
               TRANSITORY OR PROVISIONAL OR INTERIM OR IMPERMANENT OR ONETIME
               OR ONE()TIME? OR DISPOSABLE OR SHORT()(LIVED OR TERM))(2W)S1
S3        649   (INITIAL OR PRELIMINARY OR BEGINNING OR STARTING OR RUDIME-
               NTARY OR BASIC OR SIMPLE OR PRIMITIVE OR FIRST OR 1ST OR ORIG-
               INATING OR ORIGINAL OR PARTIAL OR FRACTIONAL OR UNFINISHED OR
               INCOMPLETE OR UNDEFINED OR UN()DEFINED)(2W)S1
S4          9   (("NOT" OR T OR CANNOT)(2W)(USED OR USABLE OR USEABLE OR R-
               EUSEABLE OR REUSABLE OR LIVE))(2W)S1
S5          6   (OFFLINE OR OFF()LINE)(2W)S1
S6         11   (SEED OR SEEDING)(1W)S1
S7         61   (LONG()TERM)(1W)S1
S8         11   S2:S6(30N)S7
```

8/3,K/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04940016 E.I. No: EIP98024059774
Title: Improved e-mail security protocol
Author: Schneier, Bruce; Hall, Chris
Corporate Source: Counterpane Systems, Minneapolis, MN, USA
Conference Title: Proceedings of the 1997 13th Annual Computer Security Applications Conference, ACSAC
Conference Location: San Diego, CA, USA Conference Date: 19971208-19971212
E.I. Conference No.: 47814
Source: Annual Computer Security Applications Conference 1997. IEEE Comp Soc, Los Alamitos, CA, USA,97TB100213. p 227-230
Publication Year: 1997
CODEN: CMSCE4
Language: English

Abstract: Current e-mail security systems base their security on the secrecy of the **long - term private key** . If this private key is ever compromised, all attacker can decrypt any messages - past, present, or future - encrypted with the corresponding public key. The system described in this paper uses **short term private - key** /public-key pairs to reduce the magnitude of this vulnerability. (Author abstract) 19 Refs.
Identifiers: **Long term private key** ; **Short term private key** /public key

8/3,K/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

5787723 INSPEC Abstract Number: B9802-6120B-023, C9802-6130S-022
Title: An improved e-mail security protocol
Author(s): Schneier, B.; Hall, C.
Author Affiliation: Counterpane Syst., Minneapolis, MN, USA
Conference Title: Proceedings. 13th Annual Computer Security Applications Conference (Cat. No.97TB100213) p.227-30
Publisher: IEEE Comput. Soc, Los Alamitos, CA, USA
Publication Date: 1997 Country of Publication: USA x+288 pp.
ISBN: 0 8186 8274 4 Material Identity Number: XX97-03160
U.S. Copyright Clearance Center Code: 0 8186 8274 4/97/$10.00
Conference Title: Proceedings 13th Annual Computer Security Applications Conference
Conference Sponsor: Appl. Comput. Security Associates; ACM Special Interest Group on Security, Audit, and Control
Conference Date: 8-12 Dec. 1997 Conference Location: San Diego, CA, USA
Language: English
Subfile: B C

Abstract: Current e-mail security systems base their security on the secrecy of the **long - term private key** . If this private key is ever compromised, an attacker can decrypt any messages-past, present or future-encrypted with the corresponding public key. The system described in this paper uses **short - term private - key** /public-key key pairs to reduce the magnitude of this vulnerability.

8/3,K/3 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013896613 **Image available**
WPI Acc No: 2001-380826/200140
XRPX Acc No: N01-279239
Generation method for shared secret value between entities, involves computing common shared key for each entity by combining group short term public key, intra-entity shared key, and entity long term key
Patent Assignee: CERTICOM CORP (CERT-N)
Inventor: VANSTONE S A
Number of Countries: 092 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200106697	A2	20010125	WO 2000CA838	A	20000719	200140	B
AU 200061437	A	20010205	AU 200061437	A	20000719	200140	
CA 2277633	A1	20010119	CA 2277633	A	19990719	200140	
EP 1226678	A2	20020731	EP 2000947716	A	20000719	200257	
			WO 2000CA838	A	20000719		
EP 1226678	B1	20031022	EP 2000947716	A	20000719	200373	
			WO 2000CA838	A	20000719		
DE 60006147	E	20031127	DE 606147	A	20000719	200403	
			EP 2000947716	A	20000719		
			WO 2000CA838	A	20000719		

Priority Applications (No Type Date): CA 2277633 A 19990719
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200106697	A2	E	11	H04L-009/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200061437	A			H04L-009/00	Based on patent WO 200106697
CA 2277633	A1	E		H04L-009/30	
EP 1226678	A2	E		H04L-009/00	Based on patent WO 200106697
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
EP 1226678	B1	E		H04L-009/00	Based on patent WO 200106697
Designated States (Regional): CH DE FR GB LI					
DE 60006147	E			H04L-009/00	Based on patent EP 1226678 Based on patent WO 200106697

Abstract (Basic):
... of each member. The intra-entity public key is computed for each member by mathematically combining its **short - term private key** , the **long term private key** and the intra-entity shared key...

8/3,K/4 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012890364 **Image available**
WPI Acc No: 2000-062198/200005
XRPX Acc No: N00-048724
Authenticated key agreement method between two entities in digital data communication system
Patent Assignee: CERTICOM CORP (CERT-N)
Inventor: BLAKE-WILSON S; JOHNSON D; MENEZES A; JOHNSON D B
Number of Countries: 087 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9957844	A1	19991111	WO 99CA356	A	19990503	200005	B
CA 2236495	A1	19991101	CA 2236495	A	19980501	200015	
AU 9935902	A	19991123	AU 9935902	A	19990503	200016	

EP 1075746	A1	20010214	EP 99917701	A	19990503	200111
			WO 99CA356	A	19990503	
US 20010016908	A1	20010823	US 9870794	A	19980501	200151
US 6336188	B2	20020101	US 9870794	A	19980501	200207
JP 2002514841	W	20020521	WO 99CA356	A	19990503	200236
			JP 2000547728	A	19990503	

Priority Applications (No Type Date): US 9870794 A 19980501; CA 2236495 A 19980501

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9957844	A1	E	16	H04L-009/08	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

CA 2236495	A1	E	H04L-009/30	
AU 9935902	A			Based on patent WO 9957844
EP 1075746	A1	E	H04L-009/08	Based on patent WO 9957844

Designated States (Regional): CH DE FR GB LI

US 20010016908	A1		H04L-009/30	
US 6336188	B2		H04L-009/00	
JP 2002514841	W	21	H04L-009/08	Based on patent WO 9957844

Abstract (Basic):

... The entity (i) utilizes **long term** shared **secret key** (K') to compute authenticated message on entities identity information and entities public session keys, and forwards the message to entity (j). The entity verifies the received message, and computes **short term** shared **secret key** utilizing public and private session keys of respective entities.

8/3,K/5 (Item 1 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

01660432

Method and apparatus for minimizing differential power attacks on processors

Verfahren und Vorrichtung zur Minimalisierung differentieller Stromverbrauchsangriffe

Procede et appareil de minimisation des attaques massives de type differentiel sur des processeurs

PATENT ASSIGNEE:

Certicom Corp., (2118052), 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L4W 5L1, (CA), (Applicant designated States: all)

INVENTOR:

Pezeshki, Farhad, 10 Hope Street, Toronto, Ontario M6E 1J7, (CA)

Lambert, Robert, J., 63 Holm Street, Cambridge, Ontario N3C 3N3, (CA)

LEGAL REPRESENTATIVE:

Boyce, Conor et al (74271), F. R. Kelly & Co., 27 Clyde Road, Ballsbridge , Dublin 4, (IE)

PATENT (CC, No, Kind, Date): EP 1365308 A2 031126 (Basic)

APPLICATION (CC, No, Date): EP 2003018048 000111;

PRIORITY (CC, No, Date): CA 2258338 990111

DESIGNATED STATES: DE; FR; GB

RELATED PARENT NUMBER(S) - PN (AN):

EP 1161726 (EP 2000900195)

INTERNATIONAL PATENT CLASS: G06F-001/00

ABSTRACT WORD COUNT: 122

NOTE:

Figure number on first page: 5

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 200348 648
SPEC A (English) 200348 3291
Total word count - document A 3939
Total word count - document B 0
Total word count - documents A + B 3939

...CLAIMS component s for use in a digital signature protocol where s results from an application of a **long term private key** a, and a **short term private key** k in a signing process, said method including the steps of representing said **long term private key** a as a pair of components b1)), b2)), generating a value (pi), combining said value (pi) with...

8/3,K/6 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2005 European Patent Office. All rts. reserv.

01258234
SPLIT-KEY KEY-AGREEMENT PROTOCOL
SCHLUSSELAUSTAUSCHPROTOKOLL MIT AUFGETEILTEN SCHLUSSELN
PROTOCOLE D'ACCORD DE CLE CLE FRACTIONNEE
PATENT ASSIGNEE:
Certicom Corp., (2118052), 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L4W 5L1, (CA), (Proprietor designated states: all)
INVENTOR:
VANSTONE, Scott A., 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0, (CA)
LEGAL REPRESENTATIVE:
Preuss, Udo, Dipl.-Ing. (88111), Maiwald Patentanwalts GmbH Elisenhof Elisenstrasse 3, 80335 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1226678 A2 020731 (Basic)
EP 1226678 B1 031022
WO 2001006697 010125
APPLICATION (CC, No, Date): EP 2000947716 000719; WO 2000CA838 000719
PRIORITY (CC, No, Date): CA 2277633 990719
DESIGNATED STATES (Pub A): AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; (Pub B): CH; DE; FR; GB; LI
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS B (English) 200343 515
CLAIMS B (German) 200343 515
CLAIMS B (French) 200343 549
SPEC B (English) 200343 1812
Total word count - document A 0
Total word count - document B 3391
Total word count - documents A + B 3391

...SPECIFICATION public keys of each said member,
ii. computing an intra-entity public key by mathematically combining its **short - term private key** , the **long term private key** and said intra-entity shared key;
(e) for each entity combining intra-entity public keys to derive...

...common key K.
Next, member A1)) computes a short term intra-entity public key s1))

using its **short term private key** and **long term private key** combined with a function f of the intra-entity public key, that is s1)) = x1)) + a1)) f...

...CLAIMS public keys of each said member;
(iv) computing an intra-entity public key by mathematically combining its **short - term private key** , the **long term private key** and said intra-entity shared key;
(e) for each entity combining intra-entity public keys to derive...

...to said intra-entity shared key to obtain a hashed value, multiplying said hashed value by said **long term private key** to obtain a resulting value and computing a sum of said resulting value and said **short - term private key** ..
6. A method as defined in claim 5, said group short term public key being computed by...

8/3,K/7 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00967873 **Image available**
SECURE EPHEMERAL DECRYPTABILITY
DECHIFFRABILITE EPHEMERE SURE
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 901 San Antonio Road, M/S UPAL01-521, Palo Alto, CA 94303, US, US (Residence), US (Nationality)
Inventor(s):
PERLMAN Radia J, 32 Suffolk Lane, Carlisle, MA 01741, US,
Legal Representative:
LEBOVICI Victor B (et al) (agent), Weingarten, Schurgin, Gagnebin & Lebovici, LLP, Ten Post Office Square, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 2002101974 A1 20021219 (WO 02101974)
Application: WO 2002US17344 20020531 (PCT/WO US02017344)
Priority Application: US 2001880470 20010613
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7874

Fulltext Availability:
Detailed Description

Detailed Description
... protocol, provide for authenticated,,
private, real-time communications. In the SSL protocol, a server system generates a **short - term** public/ **private key** pair that is certified as authentic using a **long - term private key** belonging to ...public key to encrypt
a symmetric key for use during the session. The server periodically changes its **short - term private key** , discarding any previous versions. This renders any records of previous sessions established using the former short-term...

8/3,K/8 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00787826 **Image available**
EPHEMERAL DECRYPTABILITY
DECHIFFREMENT EPHEMERE
Patent Applicant/Assignee:
SUN MICROSYSTEMS INC, 901 San Antonio Road, MS UPALI-521, Palo Alto, CA 94303, US, US (Residence), US (Nationality)
Inventor(s):
PERLMAN Radia J, 10 Huckleberry Lane, Acton, MA 01720, US,
Legal Representative:
LEBOVICI Victor B (et al) (agent), Weingarten, Schurgin, Gagnebin & Hayes LLP, Ten Post Office Square, Boston, MA 02109, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200120836 A2-A3 20010322 (WO 0120836)
Application: WO 2000US23997 20000831 (PCT/WO US0023997)
Priority Application: US 99395581 19990914
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 9016

Fulltext Availability:
Detailed Description

Detailed Description
... protocol, provide for authenticated, private, real-time communications. In the SSL protocol, a server system generates a **short term** public/ **private key** pair, that is certified as authentic using a **long term private key** belonging to the server.

The client uses the short term public key to encrypt a symmetric key for use during the session. The server periodically changes its **short term private key** ,, discarding any previous versions. This renders any records of previous sessions established using the former short term...

8/3,K/9 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00773169 **Image available**
SPLIT-KEY KEY-AGREEMENT PROTOCOL
PROTOCOLE D'ACCORD DE CLE CLE FRACTIONNEE
Patent Applicant/Assignee:
CERTICOM CORP, 4th Floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1, CA, CA (Residence), CA (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
VANSTONE Scott A, 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0, CA, CA (Residence), CA (Nationality), (Designated only for: US)
Legal Representative:
ORANGE John R S (et al) (agent), Orange and Chari, Suite 4900, P.O. Box 190, 66 Wellington Street W, Toronto Dominion Bank Tower,, Toronto-Dominion Center,, Toronto, Ontario M5K 1H6, CA,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200106697 A2-A3 20010125 (WO 0106697)
Application: WO 2000CA838 20000719 (PCT/WO CA0000838)
Priority Application: CA 2277633 19990719
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English

English Abstract
...term keys of each of the members computing an intra-entity public key by mathematically combining its **short - term private key** , the **long term private key** and the intra-entity shared key. Next, each entity combines intra-entity public keys to derive a...

8/3,K/10 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00493740 **Image available**
MASKED DIGITAL SIGNATURES
SIGNATURES NUMERIQUES MASQUEES
Patent Applicant/Assignee:
CERTICOM CORP,
JOHNSON Donald B,
VANSTONE Scott,
QU Minghua,
Inventor(s):
JOHNSON Donald B,
VANSTONE Scott,
QU Minghua,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9925092 A1 19990520
Application: WO 98CA1040 19981110 (PCT/WO CA9801040)
Priority Application: US 97966702 19971110
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 3477

Fulltext Availability:
  Detailed Description
  Claims

Detailed Description
... component r by using the first short term public
  key k;
  1 5 (d) generating a second **short term private key** t;
  (e) computing a second signature component s by using the second **short term private key** t on the message m, the **long term private key** and the first signature
  component r;
  (D computing a third signature component c using the first and...

Claim
... signature component r by using said first short terin public key k;
  0 (d) generating a second **short term private key** t;
  (e) computing a second signature component s by using said second **short term private key** t on said message m, said **long term private key** and said first signature
  component r;
  (f) computing a third signature component c using said first and second **short term private keys** t and k respectively, and sending said signature components (r, s, c) as a masked digital signature...

...first signature component r by using said first short term public
  key k;
  (d) generating a second **short term private key** t;
  (e) computing a second signature component s by using said second **short term private key** t on said message m, said **long term private key** and first signature
  component r;
  computing a third signature component c using said first and second **short term**
  private keys t and k respectively;
  (g) sending said signature components (r, s, c) as a masked digital signature...

8/3,K/11 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00427771 **Image available**
KEY AGREEMENT AND TRANSPORT PROTOCOL WITH IMPLICIT SIGNATURES
PROTOCOLE D'ACCORD DE CLE ET DE TRANSPORT AVEC SIGNATURES IMPLICITES
Patent Applicant/Assignee:
  CERTICOM CORP,
  VANSTONE Scott A,
  MENEZES Alfred John,
  QU Mingua,
Inventor(s):
  VANSTONE Scott A,
  MENEZES Alfred John,
  QU Mingua,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9818234 A1 19980430
  Application: WO 96US16608 19961018 (PCT/WO US9616608)
  Priority Application: WO 96US16608 19961018
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
  AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL
  IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT
  RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN KE LS MW SD SZ UG AM AZ

BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 5131

Fulltext Availability:
Detailed Description

Detailed Description
... A's and B's respective long-term private key,
aa mod p is party A's **long - term private key** ,
ab mod p is party B's **long - term private key** ,
x is a random integer selected by A as a **short - term private key** ,
ra = a' mod p is party A's short-term public key,
y is a random integer...is party A's long-term private key,
db (I<db<n-1) is party B's **long - term private key** ,
Qa = daP is party A's long-term public key,
Qb = dbp is party B's long-term public key,
k(1<k<n-1) is party A's **short - term private key** ,
ra kP is party A's short-term public key,

```
File 347:JAPIO Nov 1976-2004/Dec(Updated 050405)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200526
         (c) 2005  Thomson Derwent

Set     Items   Description
S1       4278   (PRIVATE OR SECRET)(1W)KEY? ?
S2         22   (TEMPORARY OR TRANSIENT OR INTERMEDIATE OR TRANSITIONAL OR
               TRANSITORY OR PROVISIONAL OR INTERIM OR IMPERMANENT OR ONETIME
               OR ONE()TIME? OR DISPOSABLE OR SHORT()(LIVED OR TERM))(2W)S1
S3        119   (INITIAL OR PRELIMINARY OR BEGINNING OR STARTING OR RUDIME-
               NTARY OR BASIC OR SIMPLE OR PRIMITIVE OR FIRST OR 1ST OR ORIG-
               INATING OR ORIGINAL OR PARTIAL OR FRACTIONAL OR UNFINISHED OR
               INCOMPLETE OR UNDEFINED OR UN()DEFINED)(2W)S1
S4          0   (("NOT" OR T OR CANNOT)(2W)(USED OR USABLE OR USEABLE OR R-
               EUSEABLE OR REUSABLE OR LIVE))(2W)S1
S5          1   (OFFLINE OR OFF()LINE)(2W)S1
S6          1   (SEED OR SEEDING)(1W)S1
S7        101   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)S1
S8         14   S7(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
               ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
               UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
               IV? OR CALCUL
S9       3668   PUBLIC(1W)KEY? ?
S10        10   S8 AND S9
S11        14   S8 OR S10
S12        38   (S9 OR OPEN(1W)KEY? ?)(10N)S2:S6(10N)(ESTABLISH? OR GENERA-
               T? OR CREAT???? OR FASHION? OR CONSTRUCT? OR FORM?? OR FORMING
               OR FORMATION? ? OR PRODUC????? OR DEVELOP? OR BUILT OR BUILD?
               OR COMPUTE OR COMPUTES OR COMPUTED OR COMPUTING OR DETERMIN?
               OR DISCERN?
S13        63   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)(S9 OR OPEN(1W)KEY? ?)
S14         7   S13(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR -
               FASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COM-
               PUTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DE-
               RIV? OR CALCU
S15         4   S14 NOT S11
```

11/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06156590 **Image available**
COMMUNICATION TERMINAL EQUIPMENT AND METHOD FOR CIPHER COMMUNICATION

PUB. NO.: 11-098133 [JP 11098133 A]
PUBLISHED: April 09, 1999 (19990409)
INVENTOR(s): HATASHITA MASAHIRO
APPLICANT(s): MURATA MACH LTD
APPL. NO.: 09-255100 [JP 97255100]
FILED: September 19, 1997 (19970919)
INTL CLASS: H04L-009/08; G09C-001/00; H04L-009/00; H04N-001/44

ABSTRACT

PROBLEM TO BE SOLVED: To enable simple change of set data and execute secret key mode cipher communication by providing a facsimile equipment with a means for deciphering a 2nd secret key with a 1st secret key and a **public key** and a means for ciphering data with the deciphered 2nd secret key and transmitting the result.

SOLUTION: The facsimile equipment F is provided with a means for generating a secret key and a **public key** , a means for transmitting the generated **public key** , a means for receiving ciphered data by the transmitted **public key** , and a means for deciphering the ciphered data by the secret key. These means are constituted when CPU 1 executes **public key** mode cipher algorithm stored in a ROM 3. Namely the CPU 1 **generates** the **1st secret key** and the public key and transmits the **generated** disclosed key. Then the CPU 1 controls processing for receiving the **2nd secret key** ciphered by the public key and deciphering the **2nd secret key** by the **1st secret key** . In addition, the CPU 1 ciphers data by the deciphered **2nd secret key** and transmits the ciphered data.

11/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

05756652 **Image available**
COMMUNICATION AND CERTIFICATION METHOD BY OPEN KEY CIPHER, AND DEVICE THEREFOR

PUB. NO.: 10-039752 [JP 10039752 A]
PUBLISHED: February 13, 1998 (19980213)
INVENTOR(s): TAKAGI TAKESHI
NAITO SHOZO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-189730 [JP 96189730]
FILED: July 18, 1996 (19960718)
INTL CLASS: [6] G09C-001/00; G09C-001/00; G09C-001/00; H04L-009/08; H04L-009/30; H04L-009/32
JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy)

ABSTRACT

PROBLEM TO BE SOLVED: To provide a constitution method for an open key ciphering system and device therefor which has a strength of same level or more against a complete deciphering compared with a conventional open key cipher on a rational integer ring, and has a higher strength than ever against a broadcasting attack.

SOLUTION:. A key forming device 21 **forms** prime ideals (p), (q) in an integer ring (O) on an algebraic number field for making them as a **first secret key** , and makes the remainders of their **product** (n)=(p) (q) as a first open key. Further, a **second secret key** d and a second open key e are formed from (p) and (q). A ciphering device 31 divides an inputted declarative sentence M into blocks, and ciphers them by performing a modulo ideal (n) raising operation to eth power, and outputs ciphered sentences (C(sub 0), C(sub 1),..., C(sub r-1)) to a communication path 51. A decoding device 41 decodes the inputted blocks of the ciphered sentences by performing a modulo ideal (n) raising operation to dth power, and corporates the decoded blocks of the declarative sentence for outputting the declarative sentence.

11/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

03434189 **Image available**
ACCESS CONTROL METHOD FOR IC CARD

PUB. NO.: 03-097089 [JP 3097089 A]
PUBLISHED: April 23, 1991 (19910423)
INVENTOR(s): TAKAGI SHINYA
ITO MAMORU
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD [000582] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 01-235037 [JP 89235037]
FILED: September 11, 1989 (19890911)
INTL CLASS: [5] G06K-019/073; G06F-012/14; G06K-017/00
JAPIO CLASS: 45.3 (INFORMATION PROCESSING -- Input Output Units); 30.1 (MISCELLANEOUS GOODS -- Office Supplies); 45.2 (INFORMATION PROCESSING -- Memory Units)
JOURNAL: Section: P, Section No. 1228, Vol. 15, No. 281, Pg. 136, July 17, 1991 (19910717)

ABSTRACT

PURPOSE: To detect it without transmitting secret data whether or not a terminal equipment possesses the right to transmit a command by **generating** certification information by using a **first secret key** in the terminal equipment, and inspecting the received certification information by using a **second secret key** in an IC card.

CONSTITUTION: In a terminal equipment 2, means 6-8 are provided to generate the certification information by using the first secret key in a correspondent relationship with the operation command to an IC card 1, and a means 9 is provided to transmit the operation command and the certification information to the IC card 1. In the IC card 1, a means 10 is provided to receive the operation command and the certification information, and means 11-13 are provided to inspect the certification information by using the second secret key. As long as the result of the inspection is normal, a processing is executed based on the operation command. Thus, since the certification information are transmitted and the first key itself is not transmitted between the IC card 1 and the terminal equipment 2, this key is not tapped and high-grade security can be secured

11/5/4 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014245761 **Image available**
WPI Acc No: 2002-066461/200209
XRPX Acc No: N02-049363
Electronic document signing and authentication method in internet, involves storing incomplete private keys for every user in database of

service computer cluster
Patent Assignee: NETCERTAINTY INC (NETC-N)
Inventor: ROSENBERG G
Number of Countries: 094 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200182036	A2	20011101	WO 2001US13418	A	20010426	200209	B
AU 200153809	A	20011107	AU 200153809	A	20010426	200219	

Priority Applications (No Type Date): US 2000559414 A 20000426
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200182036	A2	E	50	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200153809	A		G06F-001/00	Based on patent WO 200182036

Abstract (Basic): WO 200182036 A2
NOVELTY - A signing request transmitted from a remote user computer (104) is received at a document service computer cluster (102). The computer cluster retrieves an **incomplete private key** portion unique to the user from a private key database and **generates** a **complete private key** for signing the document.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for electronic document signing and authenticating system.
USE - For signing, storing and authenticating electronic documents such as assets rollover document, contract documents signed using **public key** cryptography for commerce, over internet.
ADVANTAGE - The user computer need not run dedicated software to enable a user to access and sign documents, as signature ready documents are signed at document service computer cluster using generated complete private key. Since only the incomplete keys are stored, security is high.
DESCRIPTION OF DRAWING(S) - The figure shows the electronic document signing and authenticating system.
Document service computer cluster (102)
Remote user computer (104)
pp; 50 DwgNo 1/11
Title Terms: ELECTRONIC; DOCUMENT; SIGN; AUTHENTICITY; METHOD; STORAGE; INCOMPLETE; PRIVATE; KEY; USER; DATABASE; SERVICE; COMPUTER; CLUSTER
Derwent Class: T01; W01
International Patent Class (Main): G06F-001/00
File Segment: EPI

11/5/5 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014191773 **Image available**
WPI Acc No: 2002-012470/200202
XRPX Acc No: N02-010297
Method of establishing secure communications link by encrypting user authorization information using shared electronic key
Patent Assignee: DEW ENG & DEV LTD (DEWE-N)
Inventor: HILLHOUSE R D
Number of Countries: 025 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1079565	A2	20010228	EP 2000118449	A	20000824	200202	B

Priority Applications (No Type Date): US 99382493 A 19990825
Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
EP 1079565 A2 E 10 H04L-009/08
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): EP 1079565 A2

NOVELTY - Method consists in transmitting a first **public key** corresponding to the first private key from the first to the second station, receiving it, along with user authorization information from the user of the second station, **determining** a shared electronic key from the first public and **second private keys**, or from the second public key corresponding to the **first** and **second private keys**, encrypting the user authorization information using the shared key, and transmitting the encrypted information and second **public key** from the second station to the first. These are received, the key is found from the second public and first private keys, user authorization information is decrypted and registered against stored data. If the user of the second station is authorized a secure communication session is initiated between the two stations.

USE - Method relates to cryptographic systems providing secure communications using an insecure network.

ADVANTAGE - Method uses authorization or biometric information to establish a secure communications link.

DESCRIPTION OF DRAWING(S) - The figure shows a flow chart of the method.

pp; 10 DwgNo 2/3

Title Terms: METHOD; ESTABLISH; SECURE; COMMUNICATE; LINK; USER; INFORMATION; SHARE; ELECTRONIC; KEY
Derwent Class: W01
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): H04L-009/32
File Segment: EPI

11/5/6 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013907397
WPI Acc No: 2001-391610/200142
XRPX Acc No: N01-288133

Information exchange public **/private** key **renewal technique having subscriber setting provisional keys/sending provisional certificate** and **certification authority sending new keys/certificate.**

Patent Assignee: SAGEM SA (SAGE)
Inventor: CHABANNE H; COURQUIN Y
Number of Countries: 025 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1096721	A1	20010502	EP 2000402951	A	20001025	200142	B
FR 2800539	A1	20010504	FR 9913426	A	19991027	200142	

Priority Applications (No Type Date): FR 9913426 A 19991027
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
EP 1096721 A1 F 5 H04L-009/30
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI
FR 2800539 A1 H04L-009/30

Abstract (Basic): EP 1096721 A1

NOVELTY - The public and private confidential key renewal technique has the subscriber setting provisional and private confidential keys and forming a provisional certificate. The provisional certificate is transmitted to the certification authority demanding key renewal. The certification authority then transmits the new defined public and

private confidential keys and the new certificate.
DETAILED DESCRIPTION - The certification authority subscriber confidential key renewal technique has the subscriber selecting **provisional** and **private keys** , and then sending a certificate to the authority. The authority replies with a new set of **defined** public and **private keys** and a new certificate.
USE - Information exchange using a certification authority with public and private keys.
ADVANTAGE - The secret of the confidentiality key is maintained during transfer from the certification authority even for the case where the old key has been compromised.
pp; 5 DwgNo 0/0
Title Terms: INFORMATION; EXCHANGE; PUBLIC; PRIVATE; KEY; RENEW; TECHNIQUE; SUBSCRIBER; SET; PROVISIONAL; KEY; SEND; PROVISIONAL; CERTIFY; CERTIFY; AUTHORISE; SEND; NEW; KEY; CERTIFY
Derwent Class: W01
International Patent Class (Main): H04L-009/30
International Patent Class (Additional): H04L-009/32
File Segment: EPI

11/5/7 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012746741 **Image available**
WPI Acc No: 1999-552858/199947
XRPX Acc No: N99-409259
Checking method for authentication and electronic signatures
Patent Assignee: STMICROELECTRONICS SRL (SGSA)
Inventor: CAPONETTO R; DI BERNARDO G; DI COLA E; OCCHIPINTI L
Number of Countries: 026 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 940675	A1	19990908	EP 98830118	A	19980306	199947	B
JP 2000112352	A	20000421	JP 9958450	A	19990305	200031	
US 6647493	B1	20031111	US 99262453	A	19990304	200382	

Priority Applications (No Type Date): EP 98830118 A 19980306
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 940675	A1	E	15	G01N-030/00	
Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 2000112352	A		40	G09C-001/00	
US 6647493	B1			H04L-009/00	

Abstract (Basic): EP 940675 A1
NOVELTY - The method involves generating an authentication and electronic signature signal using a private key. This step involves **generating** a chaotic signal based on an initial random signal. A comparison signal is **generated** using a **second private key** equal to the **first private key** , also by **generating** a chaotic signal. The comparison and signature signals are compared.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for an integrated circuit for generating an authentication and electronic signature signal, and an authentication and electronic signature system for using the method.
USE - User authentication.
ADVANTAGE - By using a chaotic generator the probability of the code being broken is reduced, e.g. improves security
DESCRIPTION OF DRAWING(S) - The figure shows an authentication system.
User smart card (1)
terminal (2)
Conventional PIN identification and checking (10,12-16)
Generation of pair of random numbers (17,18)

Both sides use chaotic generators to produce result (26,32)
Check both sides have same result (36)
pp; 15 DwgNo 1/9
Title Terms: CHECK; METHOD; AUTHENTICITY; ELECTRONIC; SIGNATURE
Derwent Class: P85; W01
International Patent Class (Main): G01N-030/00; G09C-001/00; H04L-009/00
International Patent Class (Additional): H04L-009/26; H04L-009/30; H04L-009/32
File Segment: EPI; EngPI

11/5/8 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012052556 **Image available**
WPI Acc No: 1998-469467/199841
XRPX Acc No: N98-365977

Data management system - involves transferring first and second secret-keys to users and to data centre together with user data and data content names and to confirm by scenario transferred by user whether user is authorised user

Patent Assignee: MITSUBISHI CORP (MITS)
Inventor: SAITO M
Number of Countries: 025 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 864959	A2	19980916	EP 98104490	A	19980312	199841	B
JP 10254909	A	19980925	JP 9776555	A	19970312	199849	
JP 3625983	B2	20050302	JP 9776555	A	19970312	200516	

Priority Applications (No Type Date): JP 9776555 A 19970312
Cited Patents: No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 864959	A2	E	28	G06F-001/00	
	Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI				
JP 10254909	A		21	G06F-017/30	
JP 3625983	B2		24	H04L-009/14	Previous Publ. patent JP 10254909

Abstract (Basic): EP 864959 A

The method involves transferring user data presented by a user and data content names to a key centre and to receive **first** and second secret-keys. The user data is entered as electronic watermark in a data content and is edited it in form of an edited data content. The edited data content is encrypted using the first secret-key to produce encrypted edited data content. The encrypted edited data content and the first and second secret- keys are transferred to users. A scenario of the editing process is stored. The first and **second secret - keys** are generate, to store data content names, user data, **first** and **second secret keys** and scenarios of users. The **first** and **second secret - keys** are transferred to users and to the data centre together with user data and data content names and to confirm by a scenario transferred by a user whether the user is an authorised user.

ADVANTAGE - Prevents piracy or leakage of data content using cryptography technique.

Dwg.1/4

Title Terms: DATA; MANAGEMENT; SYSTEM; TRANSFER; FIRST; SECOND; SECRET; KEY ; USER; DATA; CENTRE; USER; DATA; DATA; CONTENT; NAME; CONFIRM; TRANSFER; USER; USER; AUTHORISE; USER
Derwent Class: T01
International Patent Class (Main): G06F-001/00; G06F-017/30; H04L-009/14
International Patent Class (Additional): G06F-015/00; G06F-017/60; G09C-001/00; G09C-005/00; H04N-001/387; H04N-007/167
File Segment: EPI

11/5/9 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012050120 **Image available**
WPI Acc No: 1998-467030/199840
XRPX Acc No: N98-363861
Public key sterilization method for thwarting possible attacks - involves choosing malicious public keys , user sends information to certificate authority,certified version of public key information is sent to user and verified , another private key is calculated
Patent Assignee: CYLINK CORP (CYLI-N)
Inventor: CHEN L; WILLIAMS C S
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5796833	A	19980818	US 96718755	A	19960923	199840	B

Priority Applications (No Type Date): US 96718755 A 19960923
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5796833	A		12	H04L-009/00	

Abstract (Basic): US 5796833 A
The method involves sending the **public key** from the user to the certificate authority. Random factors are generated (31)at the certificate authority with the CA processor. Another **public key** is generated from the first **public key** and random numbers. It is difficult to compute the random numbers when the **public keys** are known.
The second **public key** is certified by generating a certificate of sterilization of the second **public key** . The certificate of the second **public key** ,a random key and additional random keys generated for calculating the second **public key** is sent from the certificate authority to the user.The user verifies the certification of the second **public key** by using a processor (21).A **second private key** using the user processor is **calculated** from the random factors , **first private key** or from second **public key** and some user's private information.
ADVANTAGE- It is practical and efficient as the **public keys** do not add on as a burden to an encryption algorithm.
Dwg.4/5
Title Terms: PUBLIC; KEY; METHOD; POSSIBILITY; ATTACK; CHOICE; PUBLIC; KEY; USER; SEND; INFORMATION; CERTIFY; AUTHORISE; CERTIFY; VERSION; PUBLIC; KEY; INFORMATION; SEND; USER; VERIFICATION; PRIVATE; KEY; CALCULATE
Derwent Class: W01
International Patent Class (Main): H04L-009/00
International Patent Class (Additional): H04L-009/30
File Segment: EPI

11/5/10 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011311657 **Image available**
WPI Acc No: 1997-289562/199726
XRPX Acc No: N97-239779
Replacement of root key used as private key of first public key -private key pair - electronically transmitting emergency message indicating that root key has been compromised and also containing replacement key, and publishing value related to message in out-of-band channel
Patent Assignee: MICROSOFT CORP (MICT)

Inventor: SPELMAN J F; THOMLINSON M W
Number of Countries: 022 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9718655	A1	19970522	WO 96US18037	A	19961114	199726	B
AU 9711185	A	19970605	AU 9711185	A	19961114	199738	
US 5680458	A	19971021	US 95555697	A	19951114	199748	
EP 861541	A1	19980902	EP 96941986	A	19961114	199839	
			WO 96US18037	A	19961114		
AU 707639	B	19990715	AU 9711185	A	19961114	199939	
JP 2001507528	W	20010605	WO 96US18037	A	19961114	200138	
			JP 97515331	A	19961114		
EP 861541	B1	20030521	EP 96941986	A	19961114	200341	
			WO 96US18037	A	19961114		
DE 6920628321	E	20030626	DE 96628321	A	19961114	200350	
			EP 96941986	A	19961114		
			WO 96US18037	A	19961114		
CA 2230630	C	20040525	CA 2230630	A	19961114	200436	
			WO 96US18037	A	19961114		

Priority Applications (No Type Date): US 95555697 A 19951114
Cited Patents: US 4799258; US 5469507; US 5499294
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9718655	A1	E	22	H04L-009/08	
Designated States (National): AU CA JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
AU 9711185	A				Based on patent WO 9718655
US 5680458	A		8		
EP 861541	A1	E			Based on patent WO 9718655
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
AU 707639	B				Previous Publ. patent AU 9711185
					Based on patent WO 9718655
JP 2001507528	W		22		Based on patent WO 9718655
EP 861541	B1	E		H04L-009/08	Based on patent WO 9718655
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
DE 6920628321	E			H04L-009/08	Based on patent EP 861541
					Based on patent WO 9718655
CA 2230630	C	E		H04L-009/08	Based on patent WO 9718655

Abstract (Basic): WO 9718655 A

The method of replacing a root key involves electronically sending out a message which indicates that the root key is being replaced. The message also contains a replacement key and a digital signature is generated by using the root key.

the replacement key is the **public key** of a second **public key** -private key pair which replaces the first such pair. A value V is published in an out-of-band channel and is related to the emergency message.

USE/ADVANTAGE - E.g. for authenticating and signing electronic documents. Central authority can use other entities to distribute emergency message rather than individually distribute message to all end users. Provision of out-of-band message along with emergency reassures users of security.

Dwg.1/4

Title Terms: REPLACE; ROOT; KEY; PRIVATE; KEY; FIRST; PUBLIC; KEY; PRIVATE; KEY; PAIR; ELECTRONIC; TRANSMIT; EMERGENCY; MESSAGE; INDICATE; ROOT; KEY; COMPROMISE; CONTAIN; REPLACE; KEY; PUBLICATION; VALUE; RELATED; MESSAGE; BAND; CHANNEL
Index Terms/Additional Words: CRYPTOGRAPHY
Derwent Class: W01
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): H04L-009/30; H04L-009/32
File Segment: EPI

11/5/11 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011201762 **Image available**
WPI Acc No: 1997-179687/199716
XRPX Acc No: N97-148055

Computational burden reduction method especially for cryptographic system - computing information that is synchronised with serial number of tamper-resistant computing device and uses it to produce output that is used to update serial number

Patent Assignee: BRANDS S A (BRAN-I)
Inventor: BRANDS S A

Number of Countries: 065 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9708870	A2	19970306	WO 96NL338	A	19960827	199716	B
AU 9667575	A	19970319	AU 9667575	A	19960827	199728	
WO 9708870	A3	19970501	WO 96NL338	A	19960827	199732	
US 5668878	A	19970916	US 94203231	A	19940228	199743	
			US 95521768	A	19950831		
US 5696827	A	19971209	US 94203231	A	19940228	199804	
			US 95521768	A	19950831		
			US 97792817	A	19970130		

Priority Applications (No Type Date): US 95521768 A 19950831; US 94203231 A 19940228; US 97792817 A 19970130
Cited Patents: EP 381523; US 5046094; US 5241598; US 5434919; WO 9525391
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9708870	A2	E	52	H04L-009/32	
	Designated States (National): AM AU BB BG BR BY CA CN CZ EE FI GE HU IS JP KG KP KR KZ LK LR LT LV MD MG MN MX NO NZ PL RO RU SG SI SK TJ TM TT UA UG US UZ VN				
	Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG				
AU 9667575	A			H04L-009/32	Based on patent WO 9708870
US 5668878	A		25	H04L-009/30	CIP of application US 94203231 CIP of patent US 5521980
US 5696827	A		25	H04L-009/30	CIP of application US 94203231 Div ex application US 95521768 CIP of patent US 5521980
WO 9708870	A3			H04L-009/32	

Abstract (Basic): WO 9708870 A

The method computes at least one number, by applying a one-way function to the second secret key and a first serial number, using a third computing device. The number is then fed to the first computing device which then computes information that is synchronised with a second serial number of the tamper-resistant computing device.

The information is fed to a second computing device which produces an output that is based on the first secret key, the information, and an application of the one-way function to at least the second secret key and the second serial number. The second computing device the updates the second serial number by applying an update function.

USE/ADVANTAGE - E.g. for electronic transfer of information against criminals who are able to gain full control of computing devices of other parties. Allows efficient **public key** cryptographic system without using special purpose cryptoprocessors. Increases security and enables currency conversion in privacy protected **public key** cryptographic systems.

Dwg.2/12

Title Terms: COMPUTATION; BURDEN; REDUCE; METHOD; CRYPTOGRAPHIC; SYSTEM; COMPUTATION; INFORMATION; SYNCHRONISATION; SERIAL; NUMBER; TAMPER; RESISTANCE; COMPUTATION; DEVICE; PRODUCE; OUTPUT; UPDATE; SERIAL; NUMBER
Derwent Class: W01

International Patent Class (Main): H04L-009/30; H04L-009/32
International Patent Class (Additional): H04L-009/08
File Segment: EPI

11/5/12 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011110678 **Image available**
WPI Acc No: 1997-088603/199709
XRPX Acc No: N97-072861

Communication system for selectively connecting multiple computers over public network - provides each transmitting and receiving computer with public network key and private key and calculates two Hash codes which are incorporated with confirmation message and encrypted with private key, respectively

Patent Assignee: PREMENOS CORP (PREM-N); JENKINS L (JENK-I); PASETES E K (PASE-I)
Inventor: JENKINS L; PASETES E K
Number of Countries: 009 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 19629192	A1	19970123	DE 1029192	A	19960719	199709	B
GB 2303525	A	19970219	GB 9614931	A	19960716	199711	
AU 9660586	A	19970123	AU 9660586	A	19960718	199712	
FR 2737067	A1	19970124	FR 969087	A	19960719	199713	
CA 2181597	A	19970120	CA 2181597	A	19960718	199721	
JP 9162860	A	19970620	JP 96221683	A	19960719	199735	
US 5812669	A	19980922	US 95503984	A	19950719	199845	
IT 1283473	B	19980421	IT 96MI1519	A	19960719	199954	
NL 1003644	C2	20000111	NL 961003644	A	19960719	200017	

Priority Applications (No Type Date): US 95503984 A 19950719
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19629192	A1		83	H04L-009/00	
GB 2303525	A		65	H04L-009/30	
JP 9162860	A		170	H04L-009/30	
NL 1003644	C2			H04L-009/32	
AU 9660586	A			H04L-009/30	
FR 2737067	A1			H04L-009/32	
CA 2181597	A			H04L-009/30	
US 5812669	A			H04L-009/00	
IT 1283473	B			H04K-000/00	

Abstract (Basic): DE 19629192 A

The communications system includes a transmitting computer which has a first associated **public** (network) **key** and a **first private key** . The receiver computer includes a second **public key** and a **second private key** . The system **calculates** a first Hash code for the electronic data interchange (EDI) from the transmitting computer.

The system then incorporates the first Hash code at a given point on the associated EDI-confirmation message. A second Hash code is computed and encrypted with the private key. Then the EDI-data is transmitted with the digital signal of the associated EDI-confirmation report. The receiving computer receives and processes the EDI-data to generate an authenticity and non-refusal or rejection of the EDI-data.

USE/ADVANTAGE - E.g for INTERNET (RTM). Enables secure electronic data exchange over open system-network.

Dwg.1/41

Title Terms: COMMUNICATE; SYSTEM; SELECT; CONNECT; MULTIPLE; COMPUTER; PUBLIC; NETWORK; TRANSMIT; RECEIVE; COMPUTER; PUBLIC; NETWORK; KEY; PRIVATE; KEY; CALCULATE; TWO; HASH; CODE; INCORPORATE; CONFIRM; MESSAGE; ENCRYPTION; PRIVATE; KEY; RESPECTIVE
Index Terms/Additional Words: EDI

Derwent Class: P85; T01; W01
International Patent Class (Main): H04K-000/00; H04L-009/00; H04L-009/30; H04L-009/32
International Patent Class (Additional): G06F-019/00; G09C-001/00; H04K-001/00; H04L-029/06
File Segment: EPI; EngPI

11/5/13 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010725316 **Image available**
WPI Acc No: 1996-222271/199622
XRPX Acc No: N96-186520
Certificate schemes based on public key cryptography - allowing triples of secret key, matching public key and secret key certificate to be generated only when certification authority involved
Patent Assignee: BRANDS S A (BRAN-I)
Inventor: BRANDS S A
Number of Countries: 065 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9612362	A2	19960425	WO 95NL350	A	19951012	199622	B
WO 9612362	A3	19960530	WO 95NL350	A	19951012	199633	
AU 9537556	A	19960506	AU 9537556	A	19951012	199636	
US 5606617	A	19970225	US 94321855	A	19941014	199714	
EP 786178	A1	19970730	EP 95935606	A	19951012	199735	
			WO 95NL350	A	19951012		
AU 705406	B	19990520	AU 9537556	A	19951012	199931	
EP 786178	B1	20020109	EP 95935606	A	19951012	200211	
			WO 95NL350	A	19951012		
DE 69524968	E	20020214	DE 624968	A	19951012	200220	
			EP 95935606	A	19951012		
			WO 95NL350	A	19951012		
JP 2002515128	W	20020521	WO 95NL350	A	19951012	200236	
			JP 96513118	A	19951012		
ES 2170167	T3	20020801	EP 95935606	A	19951012	200263	

Priority Applications (No Type Date): US 94321855 A 19941014
Cited Patents: 5.Jnl.Ref; EP 139313; No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9612362	A2	E	76	H04L-009/32	
Designated States (National): AM AU BB BG BR BY CA CN CZ EE FI GE HU IS JP KG KP KR KZ LK LR LT LU LV MD MG MN MX NO NZ PL RO RU SG SI SK TJ TM TT UA UG US UZ VN					
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT KE LU MC MW NL OA PT SD SE SZ UG					
WO 9612362	A3			H04L-009/32	
AU 9537556	A			H04L-009/32	Based on patent WO 9612362
US 5606617	A		33	H04L-009/30	
EP 786178	A1	E		H04L-009/32	Based on patent WO 9612362
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE					
AU 705406	B			H04L-009/32	Previous Publ. patent AU 9537556 Based on patent WO 9612362
EP 786178	B1	E		H04L-009/32	Based on patent WO 9612362
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE					
DE 69524968	E			H04L-009/32	Based on patent EP 786178 Based on patent WO 9612362
JP 2002515128	W		80	G09C-001/00	Based on patent WO 9612362
ES 2170167	T3			H04L-009/32	Based on patent EP 786178

Abstract (Basic): WO 9612362 A
The cryptographic method where a first party issues a certificate,

called a secret key certificate, to a second party involves a first secret key being **generated** for use by the **first** party. The **secret key** is unknown to the second party. A first public key is also **generated** . A **second secret key** is **generated** by the second party as well as a second **public key** . The first party issues a secret key certificate to the second party according to a set protocol. The certificate is generated corresp. to the second **public key** according to a publicly verifiable relation.

The secret key certificate is a digital signature of the first party on the second secret key. The second party is able to feasibly generate without assistance of the first **public key** and corresponding secret key certificates.

USE/ADVANTAGE - Allows anyone to generate **public key** and corresp. certificate, but prevents formation of triple without certification authority evolvement. Prevents **public key** directories revealing genuiness of privacy related information.

Dwg.2/12

Title Terms: CERTIFY; SCHEME; BASED; PUBLIC; KEY; ALLOW; SECRET; KEY; MATCH ; PUBLIC; KEY; SECRET; KEY; CERTIFY; GENERATE; CERTIFY; AUTHORISE
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00; H04L-009/30; H04L-009/32
File Segment: EPI; EngPI

11/5/14 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009254202 **Image available**
WPI Acc No: 1992-381619/199246
Related WPI Acc No: 1993-405278; 1995-382674; 1997-033830; 1998-506084; 1999-132651; 2000-328157; 2001-637887; 2003-066763; 2005-063917
XRPX Acc No: N92-291062

Apparatus for public key **exchange in cryptographic system - uses private and** public key **sources and two elliptic multiplying systems generating enciphering and deciphering keys**

Patent Assignee: NEXT COMPUTER INC (NEXT-N)
Inventor: CRANDALL R E
Number of Countries: 037 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5159632	A	19921027	US 91761276	A	19910917	199246	B
WO 9306672	A1	19930401	WO 92US7864	A	19920916	199314	
AU 9226977	A	19930427	AU 9226977	A	19920916	199332	
			WO 92US7864	A	19920916		

Priority Applications (No Type Date): US 91761276 A 19910917
Cited Patents: US 4200770; US 4424414; US 4567600; US 5010573; US 5054066; US 5146500; US 5159632
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5159632	A		20	H04L-009/06	
WO 9306672	A1	E	44	H04L-009/06	

Designated States (National): AT AU BB BG BR CA CH CS DE DK ES FI GB HU JP KP KR LK LU MG MN MW NL NO PL RO RU SD SE
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL OA SE

AU 9226977 A H04L-009/06 Based on patent WO 9306672

Abstract (Basic): US 5159632 A

The key **generator** for a secure key comprises a **first private key** source for providing a **first private key** ; a **second private key** source for providing a **second private key** ; and a **public key** source for providing at least first and second **public keys** . The first **public key** is generated by performing an elliptic curve. The second **public key** is generated by performing an elliptic

multiplication of the second private key and the point. The point is on an elliptic curve over a finite field FpK, where p is one of a class of numbers such that mod p arithmetic is performed in a processor using only shift and add operations.

A first elliptic multiplyer is coupled to the first private key source and the **public key** source, **generating** an enciphering key by performing an elliptic multiplication of the **first private key** and the second public key. A second elliptic multipyer is coupled to the **second private key** source and the public **key** source for **generating** a deciphering key by performing an elliptic multiplication of the second private key and the first **public key** .

ADVANTAGE - Provides faster calculations.

15/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2005 JPO & JAPIO. All rts. reserv.

08190505 **Image available**
DATA COPYRIGHT MANAGEMENT DEVICE

PUB. NO.: 2004-303265 [JP 2004303265 A]
PUBLISHED: October 28, 2004 (20041028)
INVENTOR(s): SAITO MAKOTO
MOMIKI JUNICHI
APPLICANT(s): MITSUBISHI CORP
APPL. NO.: 2004-149423 [JP 2004149423]
Division of 07-280984 [JP 95280984]
FILED: May 19, 2004 (20040519)
PRIORITY: 06-264200 [JP 94264200], JP (Japan), October 27, 1994 (19941027)
06-299835 [JP 94299835], JP (Japan), December 02, 1994 (19941202)
INTL CLASS: G06F-012/14; G06F-012/00; H04L-009/10

ABSTRACT

PROBLEM TO BE SOLVED: To provide a terminal unit for handling data copyright, digital cache and television conference system data.
SOLUTION: This data copyright management device is provided with a CPU, an ROM, an EEPROM and an RAM. The ROM, EEPROM and RAM are connected to a bus of the CPU, and a system bus of devices for using data is connectable to the bus of the CPU. A data copyright management system program, cryptographic algorithm and user information are stored in the ROM, and a second exclusive key, a use authorization key, a second private key and copyright information are stored in the EEPROM. When the device is operated, a first public key, a first exclusive key, a **second public key** and a **first private key** are transferred to the RAM. As the **form** of the data copyright management device, a monolithic or hybrid IC, a thin-type IC card or PC card with an exclusive terminal, and an insertion board are applicable and can also be built in a computer device, a television image receiver, a set-top box, digital video tape recorder, digital video disk recorder, a digital audio tape device or a portable terminal unit.

15/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2005 JPO & JAPIO. All rts. reserv.

07017295 **Image available**
SYSTEM AND METHOD FOR MANAGING ENCIPHERED DATA AND STORAGE MEDIUM

PUB. NO.: 2001-244925 [JP 2001244925 A]
PUBLISHED: September 07, 2001 (20010907)
INVENTOR(s): FUKUDA YASUO
APPLICANT(s): CANON INC
APPL. NO.: 2000-056146 [JP 200056146]
FILED: March 01, 2000 (20000301)
INTL CLASS: H04L-009/08; G06F-012/00; G06F-012/14

ABSTRACT

PROBLEM TO BE SOLVED: To manage data with high-security enciphering.

SOLUTION: Pairs of the first, **second** and third **public keys** and secret keys are **generated** and these **second** and third **public keys** and secret keys are enciphered by the **first secret key** . The enciphered

second and third **public keys** are held on the side of an authentication part and these secret keys are, respectively, passed to a client and a server. Then, data are enciphered by using the second public key on the client side (S302). These enciphered data are transmitted to the server (S304), and on the server side the enciphered data are enciphered again by using the third public key and preserved (S308).

15/5/3 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013414322
WPI Acc No: 2000-586260/200055
XRPX Acc No: N00-433804

Information handling system initialization involves receiving initialization information and accepting information based on validity of specific digital signature

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: D'AVIGNON E J; DEBELLIS R S; EASTER R J; GREEN L L; KELLY M J; SMITH R M; SPANO V A; YEH P C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6108425	A	20000822	US 97884721	A	19970630	200055	B

Priority Applications (No Type Date): US 97884721 A 19970630
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6108425	A		37	H04L-009/30	

Abstract (Basic): US 6108425 A

NOVELTY - An initialization information for information handling system is received and information is accepted based on validity of first digital signature. A message with a public verification key is received and the key is accepted based on validity of second digital signature. An additional initialization information is received and the information is accepted based on validity of third digital signature.

DETAILED DESCRIPTION - A first message containing an initialization information and a first digital signature generated on first message using a private signature key, are received. The initialization information is accepted only if first digital signature is verified as a valid signature using first public verification key. A second message containing **second public** verification **key** and a second digital signature **generated** on second message using **first private key**, are received. The **second public** verification **key** is accepted only if second digital signature is verified as valid signature using first public verification key. A third message containing additional initialization information and third digital signature generated on third message using second private signature key, are received. The additional information is accepted only if third digital signature is verified as valid signature, using second public verification key.

INDEPENDENT CLAIMS are also included for the following:

(a) program storage device;

(b) apparatus for initializing information handling system

USE - For initializing configuration of cryptographic co-processor of general purpose computer.

ADVANTAGE - Control information is in the clear and can be read and inspected. Use of crypto configuration control (CCC) provides either static or dynamic configuration control or both without requiring any changes to chip. Permits cryptographic processor to be initialized by the customer from the convenience of his own work station in his own office. Provides public access to all initialization information, thus making every step of initialization process publicity auditable.

pp; 37 DwgNo 0/38

Title Terms: INFORMATION; HANDLE; SYSTEM; RECEIVE; INFORMATION; ACCEPT; INFORMATION; BASED; VALID; SPECIFIC; DIGITAL; SIGNATURE
Derwent Class: W01
International Patent Class (Main): H04L-009/30
File Segment: EPI

15/5/4 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013051920
WPI Acc No: 2000-223775/200019
XRPX Acc No: N00-167757
Key agreement system for a two-party public and private key encryption system
Patent Assignee: CIPHERIT LTD (CIPH-N)
Inventor: ARAZI B
Number of Countries: 087 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200005836	A1	20000203	WO 99IL361	A	19990705	200019	B
AU 9945307	A	20000214	AU 9945307	A	19990705	200029	
EP 1095483	A1	20010502	EP 99928197	A	19990705	200125	
			WO 99IL361	A	19990705		

Priority Applications (No Type Date): IL 125222 A 19980706
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200005836	A1	E	25	H04L-009/08	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW

AU 9945307	A		H04L-009/08	Based on patent WO 200005836
EP 1095483	A1	E	H04L-009/08	Based on patent WO 200005836

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

Abstract (Basic): WO 200005836 A1
NOVELTY - The method provides every member (Useri) who uses the services of a Certify Authority (CA) with a public key (Pui) and a. private key (si). The process is effected over a finite group of points using the steps of permitting CA to select a generating group point (G). A random CA private key (PS) is generated (PS=dasteriskG) before permitting said member (Useri) to **generate** a random value (xi) to **calculate** a first intermediate member public key (xiasteriskG). CA **calculates** said member public key (Pui) and **intermediate private key** (pi). A second member value (yi) is **generated** and also a **second** intermediate member **public key** (yiasteriskG) to **generate** a public key Pui=xiasteriskG+yiasteriskG. A member's temporary value (H(IDi,PUi)) is formed by operating a hash transformation (H), allowing an intermediate private key (pi=H(IDi,PUi)asteriskd+yi) for member to generate private key (si) (si=pi+xi).
USE - Key agreement system for an encryption system.

```
File 348:EUROPEAN PATENTS 1978-2005/Apr W03
        (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050421,UT=20050414
        (c) 2005 WIPO/Univentio

Set     Items   Description
S1       8003   (PRIVATE OR SECRET)(1W)KEY? ?
S2         68   (TEMPORARY OR TRANSIENT OR INTERMEDIATE OR TRANSITIONAL OR
               TRANSITORY OR PROVISIONAL OR INTERIM OR IMPERMANENT OR ONETIME
               OR ONE()TIME? OR DISPOSABLE OR SHORT()(LIVED OR TERM))(2W)S1
S3        471   (INITIAL OR PRELIMINARY OR BEGINNING OR STARTING OR RUDIME-
               NTARY OR BASIC OR SIMPLE OR PRIMITIVE OR FIRST OR 1ST OR ORIG-
               INATING OR ORIGINAL OR PARTIAL OR FRACTIONAL OR UNFINISHED OR
               INCOMPLETE OR UNDEFINED OR UN()DEFINED)(2W)S1
S4          9   (("NOT" OR T OR CANNOT)(2W)(USED OR USABLE OR USEABLE OR R-
               EUSEABLE OR REUSABLE OR LIVE))(2W)S1
S5          4   (OFFLINE OR OFF()LINE)(2W)S1
S6          7   (SEED OR SEEDING)(1W)S1
S7        389   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)S1
S8         87   S7(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
               ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
               UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
               IV? OR CALCUL
S9       7865   PUBLIC(1W)KEY? ?
S10       363   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)S9
S11         4   S7(10N)S2:S6(10N)DERIV???
S12         5   S7(10N)S2:S6(10N)(DETERMIN??? OR DETERMINATION)
S13        43   (S8 OR S11:S12)(30N)S9
S14       149   S9(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
               ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
               UTES OR COMPUTED OR COMPUTING OR DETERMIN??? OR DISCERN? OR D-
               ERIV??? OR CA
S15        50   (S8 OR S11:S12)(50N)S14
S16        26   S15 AND AC=US/PR
S17        17   S16 AND AY=(1970:1999)/PR
S18        18   S15 AND PY=1970:1999
S19        21   S17:S18
```

19/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01295370
Method and apparatus for public key management
Verfahren und Vorrichtung fur offentlichem Schlusselverwaltung
Procede et dispositif pour la gestion des cles publiques
PATENT ASSIGNEE:
Nortel Networks Limited, (3029040), World Trade Center of Montreal, 380 St. Antoine Street West, 8th floor, Montreal, Quebec H2Y 3Y4, (CA), (Applicant designated States: all)
INVENTOR:
Hardjono, Thomas, 10 Fessenden Road, Arlington, MA 02476, (US)
LEGAL REPRESENTATIVE:
Coyle, Philip Aidan et al (72291), F. R. KELLY & CO. 27 Clyde Road Ballsbridge, Dublin 4, (IE)
PATENT (CC, No, Kind, Date): EP 1111873 A2 010627 (Basic)
EP 1111873 A3 030702
APPLICATION (CC, No, Date): EP 2000650209 001218;
PRIORITY (CC, No, Date): US 471554 991223
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-009/00; H04L-009/08
ABSTRACT WORD COUNT: 19
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200126	808
SPEC A	(English)	200126	2782
Total word count - document A			3590
Total word count - document B			0
Total word count - documents A + B			3590

...SPECIFICATION to a method of managing and delivering a plurality of keys in a domain. The method is **generating** a **first public / private key** pair (Pkdkd, Skdkd), a **second public / private key** pair (Pkrpbsr, Skrpbsr), and a third **public** /private **key** pair (Pkbsr, Skbsr). Configures the Pkdkd key into all routers in the domain, and the key pair ...

19/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01246952
Method of securely establishing a secure communication link via an unsecured communication network
Verfahren zum sicheren Aufbau einer sicheren Verbindung uber ein unsicheres Kommunikationsnetzwerk
Procede d'etablissement securise d'une liaison securisee par l'intermediaire d'un reseau de communication non securise
PATENT ASSIGNEE:
ACTIVCARD IRELAND LIMITED, (4032120), 30 Herbert Street, Dublin 2, (IE), (Applicant designated States: all)
INVENTOR:
Hillhouse, Robert D., 245 Irving Place, Ottawa, Ontario K1Y 1Z9, (CA)
LEGAL REPRESENTATIVE:
Colas, Jean-Pierre (14814), Cabinet JP Colas 37, avenue Franklin D. Roosevelt, 75008 Paris, (FR)
PATENT (CC, No, Kind, Date): EP 1079565 A2 010228 (Basic)

EP 1079565 A3 030402
APPLICATION (CC, No, Date): EP 2000118449 000824;
PRIORITY (CC, No, Date): US 382493 990825
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/32
ABSTRACT WORD COUNT: 141
NOTE:
Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200109	1238
SPEC A	(English)	200109	2632
Total word count - document A			3870
Total word count - document B			0
Total word count - documents A + B			3870

...SPECIFICATION a first station and a second station of a communication network. The method comprises the steps of:
generating a first private/public key pair at the first station;
signing the first public key;
transmitting the...

...at the second station;
verifying the signed first public key at the second station;
generating a second **private** /public **key** pair at the second station;

generating a shared key corresponding to the first private/public **key** pair and the **second** **private** /public **key** pair at the second station;

receiving biometric information at the second station from a user of the...

...the encrypted second public key at the first station;
decrypting the encrypted second public key using the **first** **private** **key** at the first station;
generating a shared key comprising corresponding to the **first** **private** /public **key** pair and the **second** **private** /public **key** pair at the first station;
decrypting the encrypted biometric information using the shared key at the first...

...CLAIMS first public key and a second private key wherein the shared key is also capable of being **determined** from a second public key corresponding to the second private key and the first private key;
e...

...and a second station of a communication network as defined in claim 1, wherein the first public **key** is **derived** from the **first** **private** **key** and wherein the second **public** **key** is **derived** from the second private key.
3. A method for securely **establishing** a secure communication link between a first station and a second station of a communication network as **defined** in claim 2, wherein the **first** **private** **key** is a, the first **public** **key** is **derived** using the equation ga) mod p, and the shared electronic key is z = za)) = (gb)) mod p...

19/3,K/3 **(Item 3 from file: 348)**
DIALOG(R)File 348:EUROPEAN PATENTS

01015985
GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES
GLOBALES BEDINGTES ZUGANGSSYSTEM FUR RUNDFUNKDIENSTE
ACCES CONDITIONNEL GLOBAL A DES SERVICES DE TELEDIFFUSION
PATENT ASSIGNEE:
Thomson Multimedia Inc., (4150292), 10330 North Meridian St., Indianapolis, IN 46290-1024, (US), (Proprietor designated states: all)
INVENTOR:
ESKICIOGLU, Ahmet, Mursit, 8235 Lakeshore Trail No. 125, Indianapolis, IN 46250, (US)
LEGAL REPRESENTATIVE:
Kohrs, Martin et al (88661), Thomson multimedia 46, quai A. Le Gallo, 92648 Boulogne-Billancourt Cedex, (FR)
PATENT (CC, No, Kind, Date): EP 988754 A1 000329 (Basic)
EP 988754 B1 041222
WO 1998056180 981210
APPLICATION (CC, No, Date): EP 98926327 980605; WO 98US11634 980605
PRIORITY (CC, No, Date): US 48852 P 970606
DESIGNATED STATES: DE; FR; GB; IT
INTERNATIONAL PATENT CLASS: H04N-007/167; H04N-007/16; H04N-005/00
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200452	921
CLAIMS B	(German)	200452	910
CLAIMS B	(French)	200452	1026
SPEC B	(English)	200452	3316
Total word count - document A			0
Total word count - document B			6173
Total word count - documents A + B			6173

...SPECIFICATION event of the list or guide, the digitally signed message comprises a message encrypted using a second **public** key and a digital signature created using a **first private key** . The method further comprises selecting an event from the list; receiving the digitally signed message corresponding to...

...message corresponding to each event in the guide, each of the digital certificates being encrypted using a **first** guide **private key** , the separate messages being encrypted using a smart card **public key** and containing an associated signature **created** using a **second** guide **private key** ; selecting an event from the guide; receiving the digital certificate, message and associated digital signature corresponding to...

19/3,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00981380
Method for preventing counterfeiting of articles of manufacture
Verfahren zum Verhindern von Falschungen an hergestellten Gegenstanden
Procede pour empecher la falsification d'articles de fabrication
PATENT ASSIGNEE:
PITNEY BOWES INC., (244955), World Headquarters One Elmcroft, Stamford Connecticut 06926-0700, (US), (Proprietor designated states: all)
INVENTOR:
Berson, William, 9 Huckleberry Lane, Weston, CT 06883, (US)
Zeller, Claude, 97 Fan Hill Road, Monroe, CT 06468, (US)
LEGAL REPRESENTATIVE:
Avery, Stephen John et al (47695), Hoffmann Eitle, Patent- und Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 889448 A2 990107 (Basic)

EP 889448 A3 000412
EP 889448 B1 031029
APPLICATION (CC, No, Date): EP 98112153 980701;
PRIORITY (CC, No, Date): US 886516 970701
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: G07F-007/08; G07C-001/00; G06K-019/14
ABSTRACT WORD COUNT: 122
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199901	646
CLAIMS B	(English)	200344	506
CLAIMS B	(German)	200344	492
CLAIMS B	(French)	200344	545
SPEC A	(English)	199901	2190
SPEC B	(English)	200344	2257
Total word count - document A			2836
Total word count - document B			3800
Total word count - documents A + B			6636

...CLAIMS article.
7. A method as described in Claim 6 wherein a trusted third party provides a party **producing** said label with said **first private key** and with an encryption of said first public key by a **second private key** kept secret by said trusted third party, said **producing** party including said encryption of said first public key with said label and said trusted third party...

...article.
9. A method as described in Claim 8 wherein a trusted third party provides a party **producing** said label with said **first private key** and with an encryption of said first public key by a **second private key** kept secret by said trusted third party, said **producing** party including said encryption of said first public key with said label and said trusted third party...

...CLAIMS article.
6. A method as described in Claim 5 wherein a trusted third party provides a party **producing** said label with said **first private key** and with an encryption of said first **public key** by a **second private key** kept secret by said trusted third party, said **producing** party including said encryption of said first public key with said label and said trusted third party...

19/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00902563
Secret communication and authentication scheme based on public key cryptosystem using N-adic expansion
Geheimes Kommunikations- und Authentifikationssystem unter Zugrundelegung eines Kryptosystems mit offentlichem Schlussel unter Verwendung einer n-fachen Expansi
Procede de communication et d'authentification secrete base sur un systeme cryptographique a cle secrete et utilisant une expansion n-ieme
PATENT ASSIGNEE:
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, (686339), 19-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-19, (JP), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)

INVENTOR:
Takagi, Tsuyoshi, Heidelberger Landstr. 213, 64297 Darmstadt-Eberstadt, (DE)
Naito, Shozo, 1-3-15-310, Hanakoganei Minamicho, Kodairashi, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Ritter und Edler von Fischern, Bernhard, Dipl.-Ing. et al (9672), Hoffmann Eitle, Patent- und Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 823802 A2 980211 (Basic)
APPLICATION (CC, No, Date): EP 97113746 970808;
PRIORITY (CC, No, Date): JP 96211654 960809; JP 97154095 970611; JP 97156903 970613
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04L-009/30;
ABSTRACT WORD COUNT: 176

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9807	6618
SPEC A	(English)	9807	23056
Total word count - document A			29674
Total word count - document B			0
Total word count - documents A + B			29674

...SPECIFICATION aspect of the present invention there is provided a secret communication method based on an n-adic **public** key cryptosystem using a first secret key formed by two prime numbers p and q, a second...an authenticity of an authentication message M from an encrypted authenticator based on an n-adic public **key** cryptosystem using a first secret **key** formed by two prime numbers p and q, a second secret key d, a first **public** **key** n = pq, a second **public** **key** e, and a number of partial blocks k which is an integer greater than or equal to...

...verifying an authenticity of an authentication message M from an encrypted authenticator based on an n-adic **public** **key** cryptosystem using a **first** **secret** **key** **formed** by two prime numbers p and q, a second secret key d, a first **public** **key** n = pq, a second **public** **key** e, and a number of partial blocks k which is an integer greater than or equal to...

CLAIMS 1. A secret communication method based on an n-adic **public** key cryptosystem using a first secret key formed by two prime numbers p and q, a second...an authenticity of an authentication message M from an encrypted authenticator based on an n-adic public **key** cryptosystem using a first secret **key** formed by two prime numbers p and q, a second secret key d, a first **public** **key** n = pq, a second **public** **key** e, and a number of partial blocks k which is an integer greater than or equal to...

...verifying an authenticity of an authentication message M from an encrypted authenticator based on an n-adic **public** **key** cryptosystem using a **first** **secret** **key** **formed** by two prime numbers p and q, a second secret key d, a first **public** **key** n = pq, a second **public** **key** e, and a number of partial blocks k which is an integer greater than or equal to...

19/3,K/6 (Item 6 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00899466

Method and system for depositing private key used in RSA cryptosystem
Verfahren und Einrichtung zur Ablage eines in einem RSA-Kryptosystem benutzten Geheimschlussels
Procede et dispositif de depot de cle secrete utilisee dans un systeme RSA

PATENT ASSIGNEE:
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, (686339), 19-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-19, (JP), (Proprietor designated states: all)
INVENTOR:
Obata, Masanori, 1-27-5-302, Hairando, Yokosuka-shi, Kanagawa-ken, (JP)
Sugiyama, Hiroyuki, 1950-49-4-805, Mutsuura-cho, Kanazawa-ku, Yokohama-shi, Kanagawa-ken, (JP)
Okukawa, Moribumi, 7-29-21, Higashiizumi, Nerima-ku, Tokyo, (JP)
Okamoto, Tatsuaki, 1-51-13, Nagasawa, Yokosuka-shi, Kanagawa-ken, (JP)
LEGAL REPRESENTATIVE:
von Fischern, Bernhard, Dipl.-Ing. et al (9674), Hoffmann - Eitle, Patent- und Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 821504 A2 980128 (Basic)
EP 821504 A3 001206
EP 821504 B1 031022
APPLICATION (CC, No, Date): EP 97112942 970728;
PRIORITY (CC, No, Date): JP 96197996 960726; JP 96274734 961017
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-009/08
ABSTRACT WORD COUNT: 183
NOTE:
Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199805	2235
CLAIMS B	(English)	200343	2298
CLAIMS B	(German)	200343	2195
CLAIMS B	(French)	200343	2485
SPEC A	(English)	199805	7376
SPEC B	(English)	200343	7510
Total word count - document A			9613
Total word count - document B			14488
Total word count - documents A + B			24101

...SPECIFICATION divided into two by the entity A 200 (S1), and one of the partial private keys (a **first** partial private key) is maintained at the entity A 200 (S2), while the other one of the...

...generation unit 220, using the prime numbers p and q in the deposit key information, the partial **private keys** are changed without changing the public **key** (S18), by generating a new **first partial private key** ks1' and a new second **partial private key** ks2' which satisfy the following congruence (8).

Next, a more specific example of a private key depositing...key and the second partial private key, a new first partial private key and a new second **partial private key** can be **generated** at the user's entity by using these prime numbers p and q, without changing the **public key**, so that it becomes possible to change and manage the keys easily and there is no need...

...SPECIFICATION divided into two by the entity A 200 (S1), and one of the partial private keys (a **first** partial private key) is maintained at the entity A 200 (S2), while the other one of the...generation unit 220, using the prime numbers p and q in the deposit key information, the partial **private keys** are changed without changing the public **key** (S18), by generating a new **first partial private key** ks1' and a new second **partial private key** ks2' which satisfy the following congruence (8).

Next, a more specific example of a private key depositing...

...key and the second partial private key, a new first partial private key and a new second **partial private key** can be **generated** at the user's entity by using these prime numbers p and q, without changing the **public key** , so that it becomes possible to change and manage the keys easily and there is no need...

...CLAIMS at the user's entity.
5. The method of claim 2, wherein the encryption key is the **second** partial private key itself, and the key decryption key is formed by the first partial private key...

...a new second partial private key which are different from the first partial private key and the **second partial private key** , without changing a public key of the user, by using the private key obtained from the **first partial private key** and the **second partial private key** and the prime numbers p and q delivered from said another entity.
29. A system for depositing...

...CLAIMS at the user's entity.
5. The method of claim 2, wherein the encryption key is the **second** partial private key itself, and the key decryption key is formed by the first partial private key...

...a new second partial private key which are different from the first partial private key and the **second partial private key** , without changing a public key of the user, by using the private key obtained from the **first partial private key** and the **second partial private key** and the prime numbers p and q delivered from said another entity.
29. A system for depositing...

19/3,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00862520
ROOT KEY COMPROMISE RECOVERY
RUCKGEWINNUNG EINES ANGEGRIFFENEN WURZEL-SCHLUSSELS
REPARATION DE LA COMPROMISSION D'UN CODE RACINE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Proprietor designated states: all)
INVENTOR:
SPELMAN, Jeffrey, F., 26705 N.E. Miller, Duvall, WA 98019, (US)
THOMLINSON, Matthew, W., 13158 S.E. Newport Way No. 1-201, Bellvue, WA 98006, (US)
LEGAL REPRESENTATIVE:
Franks, Robert Benjamin et al (74662), Franks & Co. 9 President Buildings Saville Street East, Sheffield South Yorkshire S4 7UQ, (GB)
PATENT (CC, No, Kind, Date): EP 861541 A1 980902 (Basic)
EP 861541 B1 030521
WO 97018655 970522
APPLICATION (CC, No, Date): EP 96941986 961114; WO 96US18037 961114
PRIORITY (CC, No, Date): US 555697 951114
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/30; H04L-009/32
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200321	1232
CLAIMS B	(German)	200321	1221
CLAIMS B	(French)	200321	1381
SPEC B	(English)	200321	4159
Total word count - document A			0
Total word count - document B			7993
Total word count - documents A + B			7993

...CLAIMS being replaced, said message also containing a replacement key (16) and a digital signature (22) which was **generated** by using the root key, said replacement key (16)being a public key of a second public...being a public key of a second public key-private key pair which is replacing the first **public key** -private key pair;
computer readable instructions for using (202) the **public key** corresponding to the root key to verify the digital signature of the message;
computer readable instructions for...

...being replaced, said message also containing a replacement key (16) and a digital signature (22) which was **generated** by using the root key, said replacement key (16) being a **public key** of a second **public key** -private key pair which is replacing the **first public key** - **private key** pair;
computer readable instructions for using (202) the **public key** corresponding to the root key to verify the digital signature of the message;
computer readable instructions for...

19/3,K/8 (Item 8 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00853936
OPTICAL DISK PROVIDED WITH BAR CODE
OPTISCHE PLATTE MIT STRICHKODE
DISQUE OPTIQUE AVEC CODE BARRES
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka-fu 571-8501, (JP), (Proprietor designated states: all)
INVENTOR:
GOTOH, Yoshiho Room 201 9-17, Higashinakahama, 4-chome Jyoto-ku Osaka-shi, Osaka 536, (JP)
OSHIMA, Mitsuaki 115-3, Minamitatsumi-cho, Katsura Nishikyo-ku Kyoto-shi, Kyoto 651, (JP)
TANAKA, Shinichi C-403, Rose Mansion, 10-1, Fukakusa Hotta-cho Fushimi-ku Kyoto-shi, Kyoto 612, (JP)
KOISHI, Kenji, 56-8, Keyakidai 3-chome Sanda-shi, Hyogo 669-13, (JP)
MORIYA, Mitsuro, 1-29, Hikarigaoka 3-chome Ikoma-shi, Nara 630-01, (JP)
LEGAL REPRESENTATIVE:
Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721), Maximilianstrasse 58, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 807929 A1 971119 (Basic)
EP 807929 A1 971210
EP 807929 B1 010228
WO 9714146 970417
APPLICATION (CC, No, Date): EP 96915172 960515; WO 96JP1303 960515
PRIORITY (CC, No, Date): JP 95261247 951009; JP 968910 960123
DESIGNATED STATES: DE; FR; GB
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1005033 (EP 101774)
EP 1005034 (EP 101775)
EP 1003162 (EP 103257)

EP 1005035 (EP 104818)
EP 1006516 (EP 105014)
EP 1006517 (EP 106447)
EP 1028422 (EP 109898)
EP 1028423 (EP 109899)
EP 1030297 (EP 110461)
EP 1031974 (EP 112310)
INTERNATIONAL PATENT CLASS: G11B-007/007; G11B-007/24; G06K-019/00; G11B-020/10; G11B-020/00; G06F-001/00
ABSTRACT WORD COUNT: 73
NOTE:
Figure number on first page: 30

LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199711W2	1907
CLAIMS B	(English)	200109	222
CLAIMS B	(German)	200109	225
CLAIMS B	(French)	200109	267
SPEC A	(English)	199711W2	24003
SPEC B	(English)	200109	2838
Total word count - document A			25916
Total word count - document B			3552
Total word count - documents A + B			29468

...SPECIFICATION PROCESS, 817. SECONDARY RECORDING PROCESS, 818. DISK MANUFACTURING PROCESS STEPS, 819. SECONDARY RECORDING PROCESS STEPS, 820. SOFTWARE **PRODUCTION** PROCESS STEPS, 830. ENCODING MEANS, 831. **PUBLIC KEY** ENCRYPTION, 833. **FIRST SECRET KEY** , 834. **SECOND SECRET KEY** , 835. COMBINING SECTION, 836. RECORDING CIRCUIT, 837. ERROR-CORRECTION ENCODER, 838. REED-SOLOMON ENCODER, 839. INTERLEAVER, 840...

19/3,K/9 (Item 9 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00807846
Method and system for generation and management of secret key of public cryptosystem
Verfahren und Einrichtung zur Erzeugung und Verwaltung eines geheimen Schlussels eines Kryptosystems mit offentlichem Schlussel
Procede et dispositif de generation et d'administration d'une cle secrete d'un systeme cryptographique a cle publique
PATENT ASSIGNEE:
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, (686339), 19-2 Nishi-Shinjuku 3-chome, Shinjuku-ku, Tokyo 163-19, (JP), (Applicant designated States: all)
INVENTOR:
Ishii, Shinji, 2-1-3-3-405, Hayashi, Yokosukashi, Kanagawaken, (JP)
LEGAL REPRESENTATIVE:
Ritter und Edler von Fischern, Bernhard, Dipl.-Ing. et al (9672), Hoffmann Eitle, Patent- und Rechtsanwalte, Arabellastrasse 4, 81925 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 750410 A2 961227 (Basic)
EP 750410 A3 000315
APPLICATION (CC, No, Date): EP 96110053 960621;
PRIORITY (CC, No, Date): JP 95155030 950621; JP 95159414 950626; JP 95204642 950810; JP 9672949 960327
DESIGNATED STATES: DE; FR; GB
RELATED DIVISIONAL NUMBER(S) - PN (AN):
EP 1175036 (EP 2001126568)
(EP 2002016802)
(EP 2002016803)

(EP 2002016804)
(EP 2002016805)
INTERNATIONAL PATENT CLASS: H04L-009/30; H04L-009/32; H04L-009/08
ABSTRACT WORD COUNT: 196
NOTE:
Figure number on first page: 1

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	5579
SPEC A	(English)	EPAB96	18471
Total word count - document A			24050
Total word count - document B			0
Total word count - documents A + B			24050

...SPECIFICATION personal portable device.
According to another aspect of the present invention there is provided a method for **generating** and managing a secret key of a public key cryptosystem, comprising the steps of: (a) separately entering...707).
When both of the verifications at the steps 701 and 702 are successful, a new partial **secret key** d(sub((0 slash) NEW)) and a new **public key** exponent e(sub(NEW)) are generated by using the new **partial secret keys** d(sub(1 NEW)) and d(sub(2 NEW)) (step 703).
Then, the secret information CardInfo stored...secret key of the public key cryptosystem to be used for deciphering the purchased digital data is **generated** and managed according to the procedure shown in the flow chart of Fig. 23 as follows. Note that this **public key** cryptosystem for deciphering is to be separately provided from the **public key** cryptosystem for signing described above.
First , the **secret key** of the pubic key cryptosystem for deciphering the purchased digital data is **generated** by the copyright owner of this digital data (step 821), and the generated secret key is strictly...

19/3,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00527051
A method for generating public and private key pairs using a passphrase.
Verfahren zur Erzeugung von offentlichen und geheimen Schlusselpaaren mittels eines Passwortes.
Procede de generation de paires de cles publiques et secretes utilisant une location de passe.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Matyas, Stephen M., 10 298 Cedar Ridge Drive, Manassas, VA 22110, (US)
Johnson, Donald B., 11 635 Crystal Creek Lane, Manassas, VA 22111, (US)
Le An V., 10 227 Battlefield Drive, Manassas, VA 22110, (US)
Martin, William C., 1835 Hilliard Lane, Concord, NC 28025, (US)
Prymak, Rostislaw, 15 900 Fairway Drive, Dumfries, VA 22026, (US)
Wilkins, John D., P.O. Box 8, Somerville, VA 22739, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 534420 A2 930331 (Basic)
EP 534420 A3 940608
APPLICATION (CC, No, Date): EP 92116309 920911;
PRIORITY (CC, No, Date): US 766533 910927
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-009/30; H04L-009/08;

ABSTRACT WORD COUNT: 216

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1819
SPEC A	(English)	EPABF1	15824
Total word count - document A			17643
Total word count - document B			0
Total word count - documents A + B			17643

...ABSTRACT A2

A data processing system, program and method are disclosed for managing a **public** key cryptographic system which includes a public key, private key pair generator. The method includes the step...

...the first public key, private key pair.

The method then continues with the step of generating a **second** public key, **private** **key** pair using a second seed value unknown to the user, the second seed value being a true random number. The second random number is generated using the second seed value in a pseudorandom number **generator** and applied to **generating** the second key pair. The method **generates** a second control vector **defining** a second use of the **second** public key, **private** **key** pair.

The method then controls the use of the **first** public key, **private** **key** pair using the first control vector and controls the use of the **second** public key, **private** **key** pair with the second control vector. (see image in original document)

...CLAIMS A3

1. In a data processing system, a method for managing a **public** key cryptographic system which includes a public key, private key pair generator, comprising the steps of:

   generating...first public key and of said first private key, respectively;

   said second generating means generating a second **public** key, private key pair using said second random number and **generating** a second public key control vector and a second private key control vector for defining a second...

...said second public key and of said second private key, respectively;

   controlling means coupled to said first **generating** means, for controlling the use of said first **public** **key** and said **first** **private** **key** using said first **public** **key** control vector and said **first** **private** **key** control vector, respectively;

   said controlling means coupled to said second **generating** means, for controlling the use of said second **public** **key** and said second private key using said second public key control vector and said second private key...

19/3,K/11 (Item 11 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00527049
Public key cryptosystem key management based on control vectors.
Schlusselverwaltung fur Geheimubertragungssystem mit offentlichem Schlussel auf Grundlage von Steuervektoren.
Administration de cle pour systeme cryptographique a cle publique basee sur des vecteurs de commande.

PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: AT;CH;DE;DK;ES;FR;GB;IT;LI;NL;SE)
INVENTOR:
Matyas, Stephen M., 10 298 Cedar Ridge Drive, Manassas, VA 22 110, (US)
Johnson, Donald B., 11 635 Crystal Creek Lane, Manassas, VA 22 111, (US)
Le, An V., 10 227 Battlefield Drive, Manassas, VA 22 110, (US)
Prymak, Rostislaw, 15 900 Fairway Drive, Dumfries, VA 22 026, (US)
Martin, William C., 1835 Hilliard Lane, Concord, NC 28 025, (US)
Rohland, William S., 4234 Rotunda Road, Charlotte, NC 28 226, (US)
Wilkins, John D., P.O. Box 8, Somerville, VA 22 739, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 534419 A2 930331 (Basic)
EP 534419 A3 940629
APPLICATION (CC, No, Date): EP 92116307 920911;
PRIORITY (CC, No, Date): US 766260 910927
DESIGNATED STATES: AT; CH; DE; DK; ES; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08;
ABSTRACT WORD COUNT: 343

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	3823
SPEC A	(English)	EPABF1	40413
Total word count - document A			44236
Total word count - document B			0
Total word count - documents A + B			44236

...ABSTRACT A2
A data processing system, method and program are disclosed, for managing a **public** key cryptographic system. The method includes the steps of generating a first public key and a first...
...second public key algorithm. The method then continues by assigning a private control vector for the first **private key** and the **second** private **key** in the data processing system, for defining permitted uses for the **first** and **second private keys** . Then the method continues by forming a private key record which includes the **first private key** and the **second private key** in the data processing system, and encrypting the private key record under a first master key expression...

...CLAIMS A3

1. In a data processing system, a method for managing a **public** key cryptographic system, comprising the steps of:

generating a first public key and a first private key...second private key in said data processing system, for defining permitted uses for said first and second **private keys** ;

key record forming means coupled to said first and second generating means, for forming a private key record which includes said **first** private **key** and said **second private** key in said data processing system, encrypting means coupled to said key record **forming** means and said assigning means, for encrypting said private key record under a first master key expression...said decryption means, for computing a second private key authentication record in said data processing system, by **computing** a second hash value using said hashing function on said decrypted private key record and comparing said **second** a **private key** authentication record with said **first private key** authentication record;

terminating means coupled to said **computing** means, for aborting further processing of said first key use request in said data processing system, if...

19/3,K/12 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00745441 **Image available**
STRUCTURE OF DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEM
STRUCTURE DE SYSTEME DE GESTION DES DROITS DE CONTENUS NUMERIQUES
Patent Applicant/Assignee:
MICROSOFT CORPORATION, One Microsoft Way, Redmond, WA 98052, US, US (Residence), US (Nationality)
Inventor(s):
PEINADO Marcus, 5007 - 148th Avenue N.E. #E207, Bellevue, WA 98007, US,
ABBURI Rajasekhar, 7844 NE 10th Street, Medina, WA 98039, US,
BELL Jeffrey R C, 107 N. 67th Street, Seattle, WA 98013, US,
Legal Representative:
ROCCI Steven J (et al) (agent), Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th floor, One Liberty Place, Philadelphia, PA 19103, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200058811 A2-A3 20001005 (WO 0058811)
Application: WO 2000US5091 20000225 (PCT/WO US0005091)
Priority Application: US 99126614 19990327; US 99290363 19990412; US 2000482932 20000113
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 22512

Fulltext Availability:
Claims

Claim
... encryption and decryption functions as part of the evaluation of any license, the black box having a **first** unique public / private key pair (PU-BB 1, PR-BB 1) that is employed I 0 as...installs the received black box on the computing device, the received black box having I 0 a **second** unique public / **private** **key** pair (PU-BB2, PR-BB2) different from the **first** unique public / **private** **key** pair (PU-BB 1, PR-BB 1).
32 The **computing** device of claim 28 wherein the license evaluator receives an enabling, valid license from the license server...decryption functions as part of the evaluation of any license with a black box having
Z:)
a **first** unique public / private key pair (PU-BB 1, PR-BB 1) that is employed as part of...

...a black box serven
receiving the requested black box; and
installing the received black box on the **computing** device. the received black box having a **second** unique public / **private** **key** pair (PU-BB2. PR-BB2) different

from the **first** unique public / **private** **key** pair (PU-BB 1. PR-BB I 5 I The method of claim 47 wherein determinincy whether...

19/3,K/13 (Item 2 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00513012 **Image available**
SYSTEM AND METHOD FOR EFFICIENT VIDEO ENCRYPTION UTILIZING GLOBAL KEY AND PARTITIONING OF DATA BLOCKS
SYSTEME ET PROCEDE DE CRYPTAGE VIDEO EFFICACE PAR UTILISATION D'UNE CLE GLOBALE ET D'UNE SEGMENTATION DE BLOCS DE DONNEES
Patent Applicant/Assignee:
CIPHERACTIVE COMMUNICATION SECURITY,
BRANDMAN Nahum,
Inventor(s):
BRANDMAN Nahum,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9944364 A1 **19990902**
Application: WO 99IL94 19990215 (PCT/WO IL9900094)
Priority Application: US 9830565 19980225
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: French
Fulltext Word Count: 6844

Patent and Priority Information (Country, Number, Date):
Patent: ... **19990902**
Fulltext Availability:
Detailed Description
Claims
Publication Year: **1999**

Detailed Description
... and decrypting data is provided. The data have a plurality of blocks. The first user has a **first** secret key, and a first public key generated from the first secret key. The second user has...have a plurality of blocks. The first user has a first secret key and a first public **key** ; the first **public** **key** is generated from the **first** secret **key** . The second user 5 has a second secret key and a second **public** **key** ; the second **public** key is **generated** from the second secret key. The system includes a first processor whichis located at the first user and a second processor which is located at the second user.
The first processor **generates** a global key from the s econd **public** **key** and the **first** **secret** **key** . The first processor scrambles and partitions a block of data to **generate** a block 0 of scrambled data having a first portion and a second portion. The first processor...

Claim
... of blocks, with each block having a multiplicity of sub-blocks, with the first user having a **first** secret key and a first public key generated from the first secret key, and with the second...encrypting and decrypting data having a plurality of blocks, with a first user having a first secret **key** and a first **public** **key** generated from the **first** **secret** **key** , and with a second user having a second secret key and a second **public** **key** **generated** from the
second secret key, comprising:

first means, located at the first user, for **generating** a global key from the second **public key** and the **first secret key** , said first means for scrambling and partitioning a block of the data, thereby **generating** a block of scrambled data having a first portion and a second portion, said first means for...

19/3,K/14 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00493740 **Image available**
MASKED DIGITAL SIGNATURES
SIGNATURES NUMERIQUES MASQUEES
Patent Applicant/Assignee:
CERTICOM CORP,
JOHNSON Donald B,
VANSTONE Scott,
QU Minghua,
Inventor(s):
JOHNSON Donald B,
VANSTONE Scott,
QU Minghua,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9925092 A1 **19990520**
Application: WO 98CA1040 19981110 (PCT/WO CA9801040)
Priority Application: US 97966702 19971110
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 3477

Patent and Priority Information (Country, Number, Date):
Patent: ... **19990520**
Fulltext Availability:
Detailed Description
Claims
Publication Year: **1999**

Detailed Description
... with this invention there is provided; a method of signing and authenticating a message m in a **public** key data communication system, comprising the steps of .

in a secure computer system.

(a) generating a first...
...in a field, the processing means comprising.

within the secure boundary;
4
means for generating a first **short term private key** ;
means for generating a second **short term private** key;
means for generating a first signature component using at least the second short
term session key; and
generating a masked signature component using the first and second short term session keys to produce masked signature...kP is converted to

an integer x, and a first signature component r = x, (mod n) is **calculated** . A second statistically unique and unpredictable integer the **second short - term private key** is selected such that 2 :5 t :5 (n-2). Second and third signature components s = t...

Claim
1 A method of signing and authenticating a message m in a **public** key data
communication system, comprising the steps of:
in a secure computer system;
(a) generating a first...first signature
component r;
computing a third signature component c using said first and second short term
private keys t and k respectively;
(g) sending said signature components (r, s, c) as a masked digital signature...

...predetermined order in a field, said processing means comprising:
within said secure boundary;
means for generating a **first short term private key** ;
means for generating a **second short term private key** ;
means for generating a first signature component using at least said second short
term session key; and
generating a masked signature component using said first and second short term session keys to produce masked signature...

19/3,K/15 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00484857 **Image available**
METHOD AND SYSTEM FOR TRANSIENT KEY DIGITAL TIME STAMPS
PROCEDE ET SYSTEME POUR HORODATEURS NUMERIQUES A CLES TRANSITOIRES
Patent Applicant/Assignee:
EOLAS TECHNOLOGIES INCORPORATED,
Inventor(s):
DOYLE Michael D,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9916209 A1 **19990401**
Application: WO 98US20036 19980922 (PCT/WO US9820036)
Priority Application: US 9759455 19970922
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM
HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO
NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE
LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR
GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 6361
Patent and Priority Information (Country, Number, Date):
Patent: ... **19990401**
Fulltext Availability:
Claims
Publication Year: **1999**

Claim
... private key for the next time interval.

8 A method for certifying data, comprising the steps of:
generating a first key pair at a first time

interval, the first key pair including a first public...first time
interval, the first key pair including a first public key and
24
a first private **key** ,
generate a second key pair at a second time
interval, the second key pair including a second public key
and a **second private key** ,
sign the second public key using the **first**
private key ,
delete the **first private key** ,
process an certification request during the
second time interval using the **second private key** , and
delete the **second private key** .

18 The system according to claim 16, wherein the general
purpose computer has a client-server architecture...

19/3,K/16 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00473179
METHOD AND APPARATUS FOR FAST ELLIPTICAL ENCRYPTION WITH DIRECT EMBEDDING
PROCEDE ET APPAREIL PERMETTANT LE CRYPTAGE ELLIPTIQUE RAPIDE PAR INTEGRATION DIRECTE
Patent Applicant/Assignee:
APPLE COMPUTER INC,
Inventor(s):
CRANDALL Richard E,
GARST Blaine,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9904531 A1 **19990128**
Application: WO 98US14892 19980717 (PCT/WO US9814892)
Priority Application: US 97896993 19970718
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
CA JP AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 18507

Patent and Priority Information (Country, Number, Date):
Patent: ... **19990128**
Fulltext Availability:
Claims
Publication Year: **1999**

Claim
... method for encrypting a plaintext message comprising the
steps of:
selecting two random numbers r and s;
generating an initial clue clueo using said random number r, a public
key from a first public key...readable program code configured to cause a
computer at said
receiver to perform the following steps of:
determining said initial clue clueo from said random number r, a
private key of said **first** public key/ **private key** pair, and a public
key of said
second public key/ **private key** pair;
determinina - which elliptic curve holds the point mi;
0
computing elliptic add(clue mi, g) to determine Xtexti; and
computing subsequent clue cluei+l usinor current clue...

19/3,K/17 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00465715 **Image available**
GLOBAL CONDITIONAL ACCESS SYSTEM FOR BROADCAST SERVICES
ACCES CONDITIONNEL GLOBAL A DES SERVICES DE TELEDIFFUSION
Patent Applicant/Assignee:
THOMSON CONSUMER ELECTRONICS INC,
ESKICIOGLU Ahmet Mursit,
Inventor(s):
ESKICIOGLU Ahmet Mursit,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9856180 A1 **19981210**
Application: WO 98US11634 19980605 (PCT/WO US9811634)
Priority Application: US 9748852 19970606
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 4389

Patent and Priority Information (Country, Number, Date):
Patent: ... **19981210**
Fulltext Availability:
Detailed Description
Publication Year: **1998**

Detailed Description
... event of the list
or guide, the digitally signed message comprises a message encrypted using a second **public** key and a digital signature created using a **first**
private **key** . The method further comprises selecting an event from the list; receiving the digitally signed message corresponding to being encrypted using a **first**
guide **private** **key** , the separate messages being encrypted using a smart card **public** **key** and containing an associated signature **created**

using a **second** guide **private** **key** ; selecting an event from the guide;
receiving the digital certificate, message and associated digital signature corresponding to...

19/3,K/18 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00456796 **Image available**
PUBLICLY VERIFIABLE KEY RECOVERY
RECUPERATION DE CLE VERIFIABLE PUBLIQUEMENT
Patent Applicant/Assignee:
NETWORK ASSOCIATES INC,
Inventor(s):
McGREW David A,
CARMAN David W,
Patent and Priority Information (Country, Number, Date):

Patent: WO 9847260 A2 **19981022**
Application: WO 98US6957 19980410 (PCT/WO US9806957)
Priority Application: US 9743766 19970411; US 9856682 19980408
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Fulltext Word Count: 15395
Patent and Priority Information (Country, Number, Date):
Patent: ... **19981022**
Fulltext Availability:
Claims
Publication Year: **1998**

Claim
... recovery information without revealing private information.

2. The method of claim 1, further comprising the steps of:
determining , by said first party, the key based on said second party's public
key and said first...said first response,
c, is said first hash of said first challenge,
k, is a first randomly **generated** integer,
y2 is said second party's **public** **key** ,
yr is the recovery agent's **public** **key** ,
x, is the **first** party's **private** **key** , and
p is a large public prime number, and
providing said first challenge, said first hash, and...said second response,
c2 is said second hash of said second challenge,
k2 is a second randomly **generated** integer,
Y2 is said second party's **public** **key** ,
y, is the recovery agent's **public** key ,
x, is the **first** party's **private** **key** , and
p is a large public prime number, and
providing said challenge, said hash, and said second...

19/3,K/19 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00377912
ROOT KEY COMPROMISE RECOVERY
REPARATION DE LA COMPROMISSION D'UN CODE RACINE
Patent Applicant/Assignee:
MICROSOFT CORPORATION,
Inventor(s):
SPELMAN Jeffrey F,
THOMLINSON Matthew W,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9718655 A1 **19970522**
Application: WO 96US18037 19961114 (PCT/WO US9618037)
Priority Application: US 95555697 19951114
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AU CA JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Publication Language: English
Fulltext Word Count: 5730

Patent and Priority Information (Country, Number, Date):
  Patent: ... **19970522**
Fulltext Availability:
  Claims
Publication Year: **1997**

Claim
... key is being replaced, said
message also containing a replacement key and a digital
signature which was **generated** by using the root key, said
replacement key being the public key of a second public
10...public key of a second public key-private key
pair which is replacing the first public key- **private** **key**
pair;
SUBSTITUTE SHEET (RULE 26)
- 19 using the public **key** of the **first** **public** **key**
private **key** pair to verify the digital signature of the
emergency message;
obtaining through an out-of-band channel...

...the emergency
message;
applying the algorithm to said at least some part
of the emergency message to **generate** a value B;
comparing B to V; and
if B equals V, replacing the **public** **key** of the
first **public** **key - private** **key** pair with the replacement
key,

11 An apparatus for recovering from a compromise
15 of a root...

19/3,K/20 **(Item 9 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00368543 **Image available**
SECURE CRYPTOGRAPHIC METHODS FOR ELECTRONIC TRANSFER OF INFORMATION
PROCEDES DE CHIFFRAGE FIABLES POUR LE TRANSFERT ELECTRONIQUE D'INFORMATIONS
Patent Applicant/Assignee:
  BRANDS Stefanus Alfonsus,
Inventor(s):
  BRANDS Stefanus Alfonsus,
Patent and Priority Information (Country, Number, Date):
  Patent: WO 9708870 A2 **19970306**
  Application: WO 96NL338 19960827 (PCT/WO NL9600338)
  Priority Application: US 95521768 19950831
Designated States:
(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)
  AM AU BB BG BR BY CA CN CZ EE FI GE HU IS JP KG KP KR KZ LK LR LT LV MD
  MG MN MX NO NZ PL RO RU SG SI SK TJ TM TT UA UG US UZ VN KE LS MW SD SZ
  UG AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM
  GA GN ML MR NE SN TD TG
Publication Language: English
Fulltext Word Count: 14910
Patent and Priority Information (Country, Number, Date):
  Patent: ... **19970306**
Fulltext Availability:
  Claims
Publication Year: **1997**

Claim
  1 A method for a user-controlled first **computing** device to reduce the

computational burden of a tamper-resistant second computing device, the second computing device...key;
computing by the first computing device, at least one output based on at least the second **secret key** and a third secret key, the first secret **key** being a function of the **second** and third **secret keys** ; and
erasing by the first computing device, the **second secret key** .

23 A method for implementing a privacy-protected off-line electronic cheque system, in which an ...the public key, the public key and the digital certificate being hidden from the issuing party, the **first secret key** comprising information certified by the issuing party, and the information certified by the issuing party comprising a **second secret key** of the first **computing** device;
receiving by the first computing device, a message speci4ring at least an amount of electronic cash...

19/3,K/21 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2005 WIPO/Univentio. All rts. reserv.

00232417
METHOD AND APPARATUS FOR PUBLIC KEY EXCHANGE IN A CRYPTOGRAPHIC SYSTEM
PROCEDE ET DISPOSITIF D'ECHANGE DE CODES PUBLICS DANS UN SYSTEME CRYPTOGRAPHIQUE
Patent Applicant/Assignee:
NEXT COMPUTER INC,
Inventor(s):
CRANDALL Richard E,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9306672 A1 **19930401**
Application: WO 92US7864 19920916 (PCT/WO US9207864)
Priority Application: US 91276 19910917
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AT AU BB BG BR CA CH CS DE DK ES FI GB HU JP KP KR LK LU MG MN MW NL NO PL RO RU SD SE AT BE CH DE DK ES FR GB GR IE IT LU MC NL SE BF BJ CF CG CI CM GA GN ML MR SN TD TG
Publication Language: English
Fulltext Word Count: 10040
Patent and Priority Information (Country, Number, Date):
Patent: ... **19930401**
Fulltext Availability:
Claims
Publication Year: **1993**

Claim
1 A key generator for **generating** a secure key comprising:
a first private key source for providing a first private key, second private...

...for providing a second private key;
public key source for providing at least first and second public **keys** ,
said first **public key** generated by performing an elliptic multiplication of said first private key and a point on an elliptic curve, and said second **public** key **generated** by performing an elliptic multiplication of said second private key and said point, said point on an...

...performed in a
processor using only shift and add operations;
first elliptic multiplying means coupled to said **first private key**

```
File 275:Gale Group Computer DB(TM) 1983-2005/Apr 27
         (c) 2005 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Apr 27
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Apr 27
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Apr 26
         (c) 2005 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2005/Apr 27
         (c)2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Apr 27
         (c) 2005 McGraw-Hill Co. Inc
File  15:ABI/Inform(R) 1971-2005/Apr 27
         (c) 2005 ProQuest Info&Learning
File 647:CMP  Computer Fulltext 1988-2005/Apr W2
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Apr W3
         (c) 2005 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2005/Apr 26
         (c) 2005 The Dialog Corp.
File 369:New Scientist 1994-2005/Mar W4
         (c) 2005 Reed Business Information Ltd.

Set     Items   Description
S1      10930   (PRIVATE OR SECRET)(1W)KEY? ?
S2         18   (TEMPORARY OR TRANSIENT OR INTERMEDIATE OR TRANSITIONAL OR
               TRANSITORY OR PROVISIONAL OR INTERIM OR IMPERMANENT OR ONETIME
               OR ONE()TIME? OR DISPOSABLE OR SHORT()(LIVED OR TERM))(2W)S1
S3         34   (INITIAL OR PRELIMINARY OR BEGINNING OR STARTING OR RUDIME-
               NTARY OR BASIC OR SIMPLE OR PRIMITIVE OR FIRST OR 1ST OR ORIG-
               INATING OR ORIGINAL OR PARTIAL OR FRACTIONAL OR UNFINISHED OR
               INCOMPLETE OR UNDEFINED OR UN()DEFINED)(2W)S1
S4          0   (("NOT" OR T OR CANNOT)(2W)(USED OR USABLE OR USEABLE OR R-
               EUSEABLE OR REUSABLE OR LIVE))(2W)S1
S5          2   (OFFLINE OR OFF()LINE)(2W)S1
S6          9   (SEED OR SEEDING)(1W)S1
S7         49   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)S1
S8          0   S7(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
               ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
               UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
               IV? OR CALCUL
S9      37886   PUBLIC(1W)KEY? ?
S10       327   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
               UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
               OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
               (2W)S9
S11         6   (LONG()TERM)(1W)S1
S12         1   S2:S6(50N)S11
S13         7   S2:S6(50N)S10
S14         7   S9(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
               ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
               PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
               UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
               IV? OR CALCUL
S15        14   S13:S14
S16         5   RD (unique items)
```

16/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02397831 SUPPLIER NUMBER: 62086503 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Broadcom Introduces the World's Fastest Processor for Network Security.(Product Announcement)
EDGE: Work-Group Computing Report, NA
May 15, 2000
DOCUMENT TYPE: Product Announcement LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 943 LINE COUNT: 00086

... 310 Mbps - 3DES, HMAC-SHA-1) performance, and in excess of 250 Diffie-Hellman key exchanges per **second** (1024-bit **public key** , 180-bit private key). Extensive hardware support for processing intensive public key operations minimizes the user software...

...TLS key negotiations. A true hardware random number generator on the BCM5805 is well suited for IV **seeding** and **secret key** generation.
The BCM5805's PCI interface makes it an optimal solution for add-in card applications. Utilizing...

16/3,K/2 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

08508709 Supplier Number: 73072339 (USE FORMAT 7 FOR FULLTEXT)
Mobile security flaw delivers yet another blow to IPv6.(Industry Trend or Event)
Marsan, Carolyn Duffy
Network World, p1
April 2, 2001
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; General Trade
Word Count: 938

... Area Co-Chair Jeff Schiller and Transport Area Co-Chairs Scott Bradner and Allison Mankin.
PBKs would **generate** a **temporary public / private key** pair to confirm that a roaming device was the same device that started a particular communication. A...

16/3,K/3 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04783079 Supplier Number: 47039952 (USE FORMAT 7 FOR FULLTEXT)
Villains in the Vault (PART TWO)
Willis, David
Network Computing, p54
Jan 15, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2495

... consolidated reporting found in RADIUS.
For a discussion of Kerberos as a method of assisting users in **establishing** encrypted communication sessions, see techweb.cmp.com/nc/801/801f1.html.
Decoding Encryption Encryption algorithms are divided into two **basic** schemes: **private key** and **public key** . Private key, or symmetric (sometimes called shared-secret), algorithms use the same key to encode and

decode...

16/3,K/4 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01596001 02-46990
Selling to Professor Plum, in the library, with a key...
Van Someren, Alex
Communications News v35n3 PP: 68-70 Mar 1998
ISSN: 0010-3632 JRNL CODE: CNE
WORD COUNT: 961

...TEXT: message itself.

This method, which has come into considerable use, is often viewed as more secure than **simple public / private key** encryption because a unique key is used to encrypt each session.

A LOT OF MATH

The **generation** of session keys and the need to re-encrypt session keys with two or more public keys...

16/3,K/5 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01116699 CMP ACCESSION NUMBER: NWC19970115S0023
State of Security - Villains in the Vault
David Willis
NETWORK COMPUTING, 1997, n 801, PG52
PUBLICATION DATE: 970115
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Features
WORD COUNT: 4834

... consolidated reporting found in RADIUS.
For a discussion of Kerberos as a method of assisting users in **establishing** encrypted communication sessions, see techweb.cmp.com/nc/801/801f1.html.
Decoding Encryption Encryption algorithms are divided into two **basic** schemes: **private key** and **public key** . Private key, or symmetric (sometimes called shared-secret), algorithms use the same key to encode and decode...

```
File   8:Ei Compendex(R) 1970-2005/Apr W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Mar
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Apr W4
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Apr W3
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Mar W2
         (c)2005 Japan Science and Tech Corp(JST)
File   6:NTIS 1964-2005/Apr W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Apr W3
         (c) 2005 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Apr W3
         (c) 2005 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Mar
         (c) 2005 The HW Wilson Co.
File 266:FEDRIP 2005/Jan
         Comp & dist by NTIS, Intl Copyright All Rights Res
File  95:TEME-Technology & Management 1989-2005/Mar W3
         (c) 2005 FIZ TECHNIK
File 438:Library Lit. & Info. Science 1984-2005/Feb
         (c) 2005 The HW Wilson Co
File  62:SPIN(R) 1975-2005/Feb W1
         (c) 2005 American Institute of Physics
File 239:Mathsci 1940-2005/Jun
         (c) 2005 American Mathematical Society

Set     Items   Description
S1       5898   (PRIVATE OR SECRET)(1W)KEY? ?
S2          4   (TEMPORARY OR TRANSIENT OR INTERMEDIATE OR TRANSITIONAL OR
                 TRANSITORY OR PROVISIONAL OR INTERIM OR IMPERMANENT OR ONETIME
                 OR ONE()TIME? OR DISPOSABLE OR SHORT()(LIVED OR TERM))(2W)S1
S3         59   (INITIAL OR PRELIMINARY OR BEGINNING OR STARTING OR RUDIME-
                 NTARY OR BASIC OR SIMPLE OR PRIMITIVE OR FIRST OR 1ST OR ORIG-
                 INATING OR ORIGINAL OR PARTIAL OR FRACTIONAL OR UNFINISHED OR
                 INCOMPLETE OR UNDEFINED OR UN()DEFINED)(2W)S1
S4          0   (("NOT" OR T OR CANNOT)(2W)(USED OR USABLE OR USEABLE OR R-
                 EUSEABLE OR REUSABLE OR LIVE))(2W)S1
S5          1   (OFFLINE OR OFF()LINE)(2W)S1
S6          3   (SEED OR SEEDING)(1W)S1
S7         30   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
                 UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
                 OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
                 (2W)S1
S8          1   S7(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
                 ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
                 PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
                 UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
                 IV? OR CALCUL
S9      17839   PUBLIC(1W)KEY? ?
S10        32   (FINAL OR FINALE OR DEFINITIVE OR DEFINITE OR DEFINED OR A-
                 UTHORITATIVE OR ENDING OR COMPLETE OR FINISHED OR TERMINATING
                 OR CONCLUDING OR CONCLUSIVE OR PERMANENT OR SECOND??? OR 2ND)-
                 (2W)S9
S11         3   S9(10N)S2:S6(10N)(ESTABLISH? OR GENERAT? OR CREAT???? OR F-
                 ASHION? OR CONSTRUCT? OR FORM?? OR FORMING OR FORMATION? ? OR
                 PRODUC????? OR DEVELOP? OR BUILT OR BUILD? OR COMPUTE OR COMP-
                 UTES OR COMPUTED OR COMPUTING OR DETERMIN? OR DISCERN? OR DER-
                 IV? OR CALCUL
S12         4   S8 OR S11
S13         4   RD (unique items)
```

13/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

6913316 INSPEC Abstract Number: C2001-06-6130S-010
Title: Key management for multilevel security in distributed applications
Author(s): Qing Si-Han; Meng Yang; Liu Ke-Long
Author Affiliation: Inst. of Software, Acad. Sinica, Beijing, China
Journal: Acta Electronica Sinica vol.29, no.2 p.269-71
Publisher: Chinese Inst. Electron,
Publication Date: Feb. 2001 Country of Publication: China
CODEN: TTHPAG ISSN: 0372-2112
SICI: 0372-2112(200102)29:2L.269:MMSD;1-#
Material Identity Number: B902-2001-004
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Applications (A); Theoretical (T)
Abstract: A key management scheme for multilevel security in distributed applications is presented. The scheme adopts the BELL-LaPadula model as multilevel access control policies. We use the Chinese Remainder Theorem, introduce the notions of **first - secret - key** -element, **second - secret - key** -element and writing-element, and **construct** sharing information of session key. The scheme is efficient, secure and dynamic. At the same time, there are many practical applications involving the scheme for key management such as meeting in the network and talking in the network etc. (8 Refs)
Subfile: C
Descriptors: access control; cryptography; distributed processing; security of data
Identifiers: multilevel security; distributed applications; key management scheme; BELL-LaPadula model; multilevel access control policies; Chinese Remainder Theorem; first-secret-key-element; second-secret-key-element; writing-element; information sharing; session key
Class Codes: C6130S (Data security); C5620 (Computer networks and techniques); C6150N (Distributed systems software); C1260C (Cryptography theory)

13/5/2 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1247210 H.W. WILSON RECORD NUMBER: BAST95042958
Cryptography is key to securing proprietary information
Watts, Antony;
EDN v. 40 (July 6 '95) p. 99-102
DOCUMENT TYPE: Feature Article ISSN: 0012-7515 LANGUAGE: English
RECORD STATUS: New record

ABSTRACT: The use of cryptography allows proprietary data to be encoded and prevents data misuse. A cryptographic system guards against threats to security by providing secrecy, integrity, and a signature to establish sender identity and confirm that an individual sent a message. There are 2 distinct groups of cryptographic schemes: secret-key and public-key methods. The secret-key algorithm is fully reversible and symmetric, which means that decrypting the cipher text yields the original plain text. Public-key systems are asymmetric, that is, the encryption and decryption algorithms are different, so passing the cipher text through the encryption stage does not **produce** the **original** message. **Secret - key** systems have enjoyed greater use than **public - key** systems, despite the significant advantages available with **public - key** cryptography. **Public - key** systems need considerably more computational resources to match the encryption and decryption speeds of secret-key systems and therefore cost a lot more.

DESCRIPTORS: Cryptographic keys; Encryption algorithms;

13/5/3 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci

03685680 MR 2005f#94076
Certificateless public key cryptography.
Advances in cryptology---ASIACRYPT 2003
Al-Riyami, Sattam S. (Information Security Group, Royal Holloway and Bedford New College, Egham, TW20 0EX, England)
Paterson, Kenneth G. (Information Security Group, Royal Holloway and Bedford New College, Egham, TW20 0EX, England)
Corporate Source Codes: 4-LNDHB-IS; 4-LNDHB-IS
2003,
Springer, Berlin,; 452--473,,
Series: Lecture Notes in Comput. Sci., 2894,
Language: English Summary Language: English
Document Type: Proceedings Paper
Journal Announcement: 200503
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: LONG (68 lines)
In this paper the concept of certificateless public key cryptography (CL-PKC) is introduced. This CL-PKC does not need the use of digital certificates as in the traditional public key infrastructure (PKI). Hence, this model for the use of public key cryptography can be considered to be between traditional PKI and identity-based public dey cryptography (ID-PKC) [A. Shamir, in Advances in cryptology (Santa Barbara, Calif., 1984), 47--53, Lecture Notes in Comput. Sci., 196, Springer, Berlin, 1985; \refcno 820012\endrefcno].

The CL-PKC makes use of a trusted third part, which is called the key generating center (KGC). Given a user A with an identifier $ID\sb A$, the KGC computes, from $ID\sb A$ and a master-key, a partial private key $D\sb A$ which is provided securely to A. Then, the entity A combines its partial private key $D\sb A$ with some secret information to generate its actual private key $S\sb A$. In this way, $S\sb A$ is not accessible to KGC. Later, A uses its secret information with the KGC's public parameters to generate its public key $P\sb A$.

An adversary could replace A's public key by a false key, but this adversary does not gain anything since A's correct private key requires for its **generation** the **partial private key** which is provided by KGC.

The certificateless **public key** encryption (CL-PKE) scheme is specified by seven randomized algorithms: (1) The setup algorithm takes a secure parameter to return the system parameters, which will be publicly known, and the master-key. (2) The partial-private-key-extract algorithm takes as input the system parameters, the master-key, and $ID\sb A$, to return $D\sb A$. These two algorithms are run by the KGC, whereas the next three algorithms are run by the entity A. (3) The set-secret-value algorithm considers as input the system parameters and $ID\sb A$ to output A's secret value $x\sb A$. (4) The set-private-key algorithm takes the system parameters, $D\sb A$, and $x\sb A$, and returns the private key $S\sb A$. (5) The set-public-key algorithm considers the system parameters and $x\sb A$ as input and returns A's public key $P\sb A$. The next two algorithms permit encryption and decryption of messages. (6) The encrypt algorithm takes as input the system parameters, a message, the public key $P\sb A$, and the identifier $ID\sb A$ of A, and returns either a ciphertext or a null symbol if the encryption procedure fails. Finally, (7) the decryption algorithm returns the original message or a null symbol if the decryption procedure fails, from an input of the ciphertext, the system parameters, and the private key $S\sb A$.

After introducing CL-PKE, the authors define and discuss the possible actions that an adversary can carry out against the CL-PKE.

Then, they describe a pair of CL-PKE schemes based on bilinear maps, which are analogous to those presented in [D. Boneh and M. Franklin, in i Advances in cryptology---CRYPTO 2001 (Santa Barbara, CA), 213--229, Lecture Notes in Comput. Sci., 2139, Springer, Berlin, 2001; \refmr MR1931424 (2003h:94054)\endrefmr]. Moreover, the authors prove that these CL-PKE schemes are secure assuming that the generalized bilinear Diffie-Hellman problem (GBDHP) is hard, where GBDHP is defined in the following way. Let $G\sb 1$ be an additive group of prime order q, P a generator of $G\sb 1$, $G\sb 2$ a multiplicative group of the same order, and a map $e\colon G\sb 1 \times G\sb 1\rightarrow G\sb 2$, such that: (1) e is bilinear, i.e., given $Q,W,Z\in G\sb 1$, then $e(Q,W+Z) =e(Q,W)\cdot e(Q,Z)$ and $e(Q+W,Z)=e(Q,Z)\cdot e(W,Z)$, (2) e is nondegenerate, i.e., $e(P,P)\neq 1\sb {G\sb 2}$, and (3) the map e is efficiently computable. The GBDHP in $\langle G\sb 1,G\sb 2,e\rangle$ is as follows: Given $\langle P,aP,bP,cP\rangle$ with uniformly random choices of $a,b,c\in Z\sb q\sp {\ast}$, output a pair $\langle Q\in G\sb 1\sp {\ast},e(P,Q)\sp {abc}\in G\sb 2\rangle$.

Finally, a certificateless signature scheme is presented.

\{For the entire collection see MR 2005d:94150.\}

Reviewer: Hernandez Encinas, Luis (E-CSIC-FA)

Review Type: Signed review

Proceedings Reference: 2005d#94150; 2 094 316

Descriptors: *94A60 -Information and communication, circuits-Communication, information-Cryptography (See also 11T71, 14G50, 68P25) ; 94A62 -Information and communication, circuits-Communication, information-Authentication and secret sharing

13/5/4 (Item 2 from file: 239)

DIALOG(R)File 239:Mathsci

02944869 MR 99j#94055

Cryptography and number theory.

Morales-Luna, Guillermo (Seccion de Computacion, Departamento Ingenieria Electrica, National Polytechnic Institute, 07738 Mexico DF, Mexico)

Vazquez Garcia, Fernando (Seccion de Computacion, Departamento Ingenieria Electrica, National Polytechnic Institute, 07738 Mexico DF, Mexico)

Corporate Source Codes: MEX-IPN-CP; MEX-IPN-CP

Miscelanea Mat.

Miscelanea Matematica, 1989, No. 18 25--54.

Language: Spanish Summary Language: Spanish

Document Type: Journal

Journal Announcement: 9908

Subfile: MR (Mathematical Reviews) AMS

Abstract Length: SHORT (10 lines)

Summary (translated from the Spanish): ``We present numerical message encryption systems, **first secret - key** systems and then **public - key** systems. For the **former** , the coding and decoding processes can be carried out easily when their respective keys are known. For the latter, the decoding of messages remains a difficult problem even when the keys are known. Some of latter methods are based on the difficulties connected with the factoring of large integers and with deciding whether a large integer is a prime. We present methods for treating these problems.''